Is Microsoft Trying to Kill Windows Server?

Windows IT Pro

A PENTON PUBLICATION

SEPTEMBER 2012 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

Exchange Server 2013 Preview

Enhanced management, data leak protection, team mailboxes, modern public folders, and more

High Availability for File Shares

Windows Server 2012 Arrives

Hiding Active Directory Objects and Attributes

Generate Random Passwords in PowerShell

Plus >>

MATCH YOUR SERVER TO YOUR BUSINESS.

ONLY PAY FOR WHAT YOU NEED!

With a 1&1 Dynamic Cloud Server, you can change your server configuration in real time.

- Independently configure CPU, RAM, and storage
- Control costs with pay-per-configuration and hourly billing
- Up to 6 Cores, 24 GB RAM, 800 GB storage
- 2000 GB of traffic included free
- Parallels® Plesk Panel 10 for unlimited domains, reseller ready
- Up to 99 virtual machines with different configurations

1&1 DYNAMIC CLOUD SERVER

SAVE $180

$34.99/ month first year, base configuration only (regularly $49.99).

- **NEW:** Monitor and manage your cloud server through 1&1 mobile apps for Android™ and iPhone®.

MEMBER OF united internet

www.1and1.com

1&1®

*Offer valid for a limited time only. First year $34.99/ month only applies to base configuration. Base configuration includes 1 processor core, 1 GB RAM, 100 GB Storage. Other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet, all other trademarks are the property of their respective owners.

BUILT FOR THE HUMAN NETWORK CISCO.

YOUR BUSINESS NEEDS TO BE AGILE, FLEXIBLE AND RESILIENT. SO WHY IS YOUR SERVER ARCHITECTURE STATIC, COMPLEX AND OUTDATED?

When we designed our servers, we started fresh. No silos, no complexity. The result is a server unlike any other on the market. It's the Cisco Unified Computing System™. And it transforms efficiency and productivity. That's because Cisco UCS is based on simplicity, integration, speed, automation and ease. It's a difference our customers are noticing: 80% increase in administrator productivity. 90% reduction in deployment times. 40% improvement in application performance. 30% lower infrastructure costs. No wonder over 11,000 businesses have purchased Cisco UCS. It's built for productivity. Built for the future. Built by the only company in the world that could. Learn more at cisco.com/servers.

Cisco UCS is powered by the Intel® Xeon® processor.

SEPTEMBER 2012 / VOL. 18 / NO. 9

COVER STORY ▼

Exchange Server 2013 Preview

— Tony Redmond

Microsoft will release Exchange Server 2013 as part of its Wave 15 release of Office application servers in early 2013. Exchange 2013 represents three years of output and includes numerous changes, improvements, and tweaks.

55

Features

Special Feature

Interact

In Every Issue

Chat with Us

Facebook Twitter LinkedIn

Columns

Products

Windows IT Pro, September 2012, Issue No. 217, ISSN 1552-3136. *Windows IT Pro* is published monthly by Penton Media, Inc.

Windows IT Pro, 748 Whalers Way, Fort Collins, CO 80525, 800-621-1544 or 970-663-4700. Customer Service: 800-793-5697.

We welcome your comments and suggestions about the content of *Windows IT Pro*. We reserve the right to edit all submissions. Letters should include your name and address. Please direct all letters to letters@windowsitpro.com. IT pros interested in writing for *Windows IT Pro* can submit articles to articles@windowsitpro.com.

WINCONNECTIONS: OCT 29 - NOV 1 • BELLAGIO • LAS VEGAS

CLOUD CONNECTIONS | WINDOWS CONNECTIONS | Microsoft Exchange CONNECTIONS | SQL Server CONNECTIONS | SharePoint CONNECTIONS

KEYNOTES

PAUL THURROTT
WINDOWS IT PRO
Senior Technical Analyst

JEFFREY SNOVER
MICROSOFT
Distinguished Engineer and the Lead Architect for Windows Server

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

MARY JO FOLEY
ALL ABOUT MICROSOFT
Editor

the JOURNEY CONTINUES

Join Microsoft & Industry Experts as they **Help you Navigate** *the new and Exciting Technologies & Releases*

Hear what past attendees are saying about Connections...

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

Is Microsoft Trying to Kill Windows Server?

The Metro-style UI is a barrier to adoption of Windows Server 2012

I've been using first the Window Server 8 and then the Windows Server 2012 prereleases for a while now, and the enthusiasm I had with the earlier release has definitely been dampened by the new Windows Server 2012 Release Candidate (RC). I've come away from the RC with very mixed feelings. On one hand, I'm still blown away by many of the new features, such as Windows Server 2012 Hyper-V, the new Resilient File System (ReFS), Server Message Block (SMB) 3.0, and the new built-in NIC teaming. But on the other hand, I can't believe Microsoft would saddle Server 2012 with the Metro-style UI without providing the traditional Windows desktop-style UI option.

Earlier versions of Server 2012 provided both interfaces. But with the RC, Microsoft dropped the traditional Windows desktop UI in favor of the Metro-style UI. That's right, Metro on the server. Don't get me wrong. I think Metro is great on the phone and on the tablet and eventually might be a good choice for the desktop. But it's definitely not a good choice for servers. For the sake of full disclosure, I'll admit I don't like the Metro-style UI on a desktop that doesn't support touch, either. Personally, I find Metro to be flat, one-dimensional, somewhat garish, and even ugly when compared with the more elegant Windows Aero UI. I definitely don't care for Metro on the server, and I can see from the comments on Microsoft's Windows Server 2012 forums that I'm not alone in this sentiment. I like Metro on the tablet, and I plan on getting one of the new Surface models. But I don't think a touch screen belongs on a server, and it doesn't work well there.

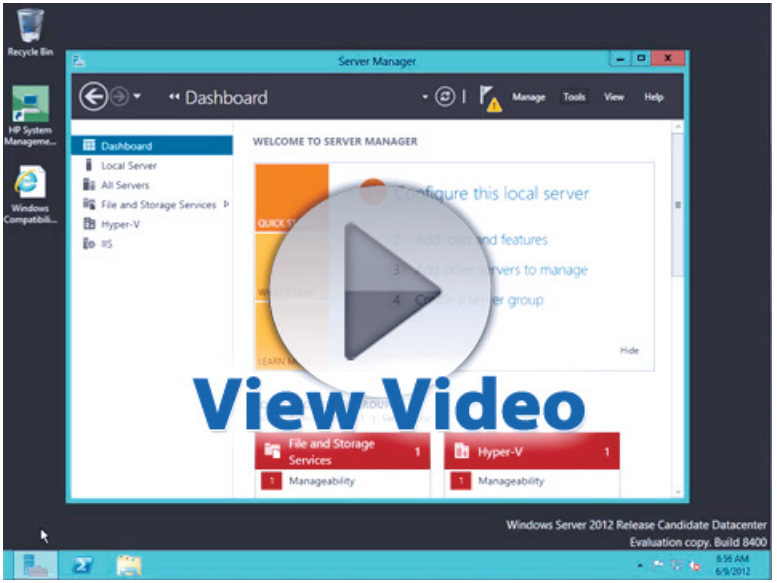
Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

Video

Michael Otey shares his thoughts about the Metro-style UI



If Microsoft is trying to discourage users from using the GUI, the company has certainly found a way to do so. However, Microsoft has also put up a huge, unnecessary hurdle for the adoption of Server 2012. Metro is really about enabling touch interface and then hopefully also providing a usable desktop interface. A touch interface just doesn't make sense on a server. Today's servers don't have touch-enabled hardware and won't for years to come. Making Metro available as an optional feature is a win-win solution, but making it the only option certainly isn't.

I'm sure Microsoft has reasons for its decision. However, from my perspective there are so many things wrong with this choice that I'm not even sure where to start. First and foremost, Metro does absolutely nothing to facilitate the server management experience. In fact, it gets in the way and isn't nearly as effective as the old Start button. There's a definite learning curve. For example, hovering the mouse in the upper right corner to make your menu options appear isn't intuitive. And trying to hit that spot on a slow RDP link is challenging. In addition, Metro forces way more mousing and clicking than the old Start button required.

The main problem I have with Metro is the lack of visibility. The new Start menu doesn't show all your programs. You can start programs by trying to type in their name and hope you guess correctly. If you haven't used Metro, then you might get the mistaken impression that it's unusable. That's not the case. It's usable. Common tasks are on the Start menu. However, the Start menu is flat and not hierarchical, so it gets super cluttered if you try to add everything you want to it.

I suppose you could say there are other interface options. Microsoft has provided a minimal UI that you can get by removing the Server Graphical Shell feature. That interface gives you Server Manager and the Windows command shell, which seems odd—perhaps even ironic—given Microsoft's strong encouragement to use PowerShell. You sort of have to wonder about the message here. Microsoft pushes Metro as the superior GUI interface on the graphical shell installation. But on the minimal interface, you get the old Windows command shell, implying that it's superior to PowerShell. I just don't get these choices. But I digress.

I realize the goal is to push IT pros to manage servers with PowerShell. But Microsoft really should face facts. Most people don't use PowerShell now. Forcing people to use it with an ineffective UI isn't the best approach. PowerShell might indeed be the better management option. But most people manage Windows Server using the GUI. Metro should be an optional alternative to the more familiar traditional Windows desktop UI. That approach would have been a win-win solution for Microsoft and its customers. Users who want Metro could have it, whereas those who don't wouldn't be forced to use it and could be immediately productive with the interface they know. Why burden an otherwise fantastic release with a UI that's clearly not designed for a server? OK, Microsoft isn't trying to kill Windows Server with Metro. But Metro is an unnecessary stumbling block for the adoption of Server 2012. ■

InstantDoc ID 143747

Letters

An Update on Windows Server 2012 Hyper-V

I just read Michael Otey's article "Get Ready for Windows Server 2012 Hyper-V," and I noticed this comment and these scalability numbers:

> This trend is sure to continue as the upcoming Windows Server 2012 Hyper-V essentially draws even with vSphere in feature parity. For scalability, Server 2012 Hyper-V supports 160 cores and 2TB of RAM per host. It will also support 64 vCPUs and 1TB of RAM per VM. Other important new capabilities will include 64-node clusters, shared-nothing Live Migration, Hyper-V Replica, and built-in NIC teaming.

I just wanted to let you know that Microsoft has consistently increased scale at the Beta and now the Windows Server 2012 Release Preview. The numbers are substantially higher than Michael reported. Server 2012 Hyper-V now supports 320 cores and 4TB of RAM per host.

Michael also states that Hyper-V "draws even with vSphere." I want to respectfully point out that Server 2012 Hyper-V far surpasses VMware vSphere across the board. For a detailed comparison, see the white paper "Why Hyper-V? Competitive Advantages of Windows Server 2012 Release Candidate Hyper-V over VMware vSphere 5.0."

Finally, in Brad Anderson's keynote at TechEd Europe, I demonstrated—for the first time—a single virtual machine (VM) delivering more than 1 million I/O operations per second (IOPs). For context, VMware claims that it can deliver up to 300,000 IOPs from a single VM and needs six VMs to achieve 1 million. Microsoft can do it with one VM in Server 2012.

My demo begins at 58 minutes into the video, and Figure 1 shows a photo sent to me by someone in the audience. That's industry-standard

Send Your Comments

Windows IT Pro welcomes feedback about the magazine. Send comments, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Comments 

Figure 1
Microsoft demo

Hyper-V Host Scale and Scale-Up Workload Support

System	Resource	Maximum number		Improvement factor
		Windows Server 2008 R2	Windows Server 2012	
Host	Logical processors per server	64	**320**	5×
	Physical memory	1TB	**4TB**	4×
Virtual machine	Virtual processors per VM	4	**64**	16×
	Memory per VM	64GB	**1TB**	16×
	Capacity per virtual disk	2TB	**64TB**	32×
Cluster	Nodes	16	**64**	4×
	Simultaneous Live Migration	1	**Unlimited**	-
	Shared Nothing Live Migration	No	**Yes**	-
Perf	Input/Output Operations per Second (IOPs)	300,000	**1,000,000+**	3×+

Table 1
Hyper-V improvements

Iometer showing 1,026,026 IOPs. I even detailed all the hardware used in the demo in the keynote. Finally, Table 1 shows you just a few of the improvements since our last release.

—Jeff Woolsey, principal program manager lead, Windows Server and cloud, Microsoft

Off the Mark on SBS

Although I enjoy Paul Thurrott's honest and typically well-informed and incisive commentary about Microsoft products, I have to say that his WinInfo Short Takes commentary "Microsoft Kills Windows Home and Small Business Server . . . But Fans Only Care About the Former" is off the mark regarding Small Business Server (SBS).

SBS 2011 had two versions: SBS 2011 Essentials, which isn't going anywhere, and SBS 2011 Standard, which is indeed outdated and will be dropped. Windows Server 2012 Essentials is a continuation/upgrade of SBS 2011 Essentials. I think SBS 2011 Standard will be missed by a large number of partners and by end users. They might not mourn the product name but rather the lack of a relatively low-cost on-premises solution. Server 2012 Essentials will handle only up to 25 users. What if you have a 40-user business that needs Active Directory (AD) and has inferior broadband? You'll potentially be forced to buy full Windows Server and potentially Exchange Server Standard Edition and pay more for services.

SBS was always about choice. Although I agree with Paul that Server 2012 Essentials is a great hybrid solution, limiting it to 25 users leaves a lot of customers out in the cold. ■

—Mark Mulvany

InstantDoc ID 143794

Microsoft Surface, Windows Phone 8 and 7.8, and the Latest Windows OSs

It's been an amazing summer for Microsoft, with back-to-back announcements spanning a wide range of products and product categories. And if you thought news of the Windows 8 Release Preview and Windows Server 2012 Release Candidate was big, well, hang on to your hats. Microsoft is just getting started.

Paul Thurrott

is senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows, a weekly editorial for Windows IT Pro UPDATE, and a daily Windows news and information newsletter called WinInfo Daily UPDATE.

Email

Twitter

Website

Microsoft Surface

In mid-June, Microsoft invited journalists and tech bloggers to a mysterious, invitation-only event in Los Angeles but wouldn't provide any details. It was a blockbuster: At the event, Microsoft announced that it was getting into the PC hardware business for the first time and was launching a new series of devices branded as Surface (see Figure 1).

Yes, it's the same name that was previously used by a niche lineup of touch-based tablets. The first two new Surface products, called Surface for Windows RT and Surface for Windows 8, are nearly identical-looking slate tablet devices. And they are incredible.

The devices run on completely different architectures, with the Windows RT version using an NVIDIA Tegra 3–based ARM architecture and the Windows 8 version being a typical Intel-based PC with Core i5 innards; the Windows 8 version comes with Windows 8 Pro, not the "Core" version of Windows 8. They both utilize 10.6" widescreen displays, with a unique new VaporMg form factor, incorporating a built-in kickstand. From there, however, the specs differ.

The Windows RT version is thinner (9.3mm) and lighter (about 1.5 pounds) than the Windows 8 version, which comes in at 13.5mm and is just a hair under 2 pounds. The RT version will likely be quieter as

Figure 1
Microsoft Surface

well, since it has no fans, but Microsoft is touting a unique, edge-based cooling system for the Windows 8 version that could be effective.

The Windows RT version utilizes an HD screen running at 1366 × 768, ideal for Metro, including side-by-side app "snap" support. But the Windows 8 version hits full HD, with 1920 × 1080, a high DPI wonder that Apple would feel comfortable calling a "Retina" display. From there, the other differences range from understandable to weird: The Windows RT version comes in variants with 32GB or 64GB of Flash-based storage, while the Windows 8 version sports 64GB or 128GB of storage. The Windows RT ports include microSD, USB 2.0, micro HDMI video out, and dual MIMO antennae, but the Windows 8 ports are microSDXC, USB 3.0, mini DisplayPort video out, and dual MIMO antennae. The Windows 8 version includes a stylus for tablet PC–style note taking and drawing with handwriting recognition.

Both Surface devices offer a choice of two keyboard cover types, Touch and Type, the former of which comes in several colors. The Touch Cover is an ultra-thin (3mm) cover with integrated keyboard and, believe it or not, multi-touch track pad. The slightly thicker Type Cover is for those who require a more traditional typing experience.

Microsoft says that the RT version of Surface will ship when Windows 8 and Windows RT become generally available (in September or October 2012), and the Windows 8 version will ship 90 days later. Although there's no explanation for that little delta, this is only the tip of the iceberg when it comes to examining Surface. Obvious questions include how much the devices will cost, whether this move will harm Microsoft's relationship with hardware partners, and whether Surface can succeed where most Microsoft hardware—sans the Xbox 360—has failed.

But no matter. With Surface, Microsoft has injected a sense of excitement and made Windows 8—and Windows RT—suddenly very interesting indeed.

Windows Phone 8

Microsoft will deliver Windows Phone 8 in late 2012 alongside Windows 8 and Server 2012. It's based on the same code base as those products, which is rather amazing, utilizing the same kernel, networking stack, security, sensors, multimedia platform, web browser, and other components as Windows 8 and Windows RT. Although it will run existing Windows Phone 7.x apps and games, it also will support new WinRT- and DirectX-based apps and games that are somewhat compatible with those for Windows 8—a brave new world indeed.

The issue, such as it is, is that Windows Phone 8 won't run on existing Windows Phone handsets. So a new generation of hardware devices will be required, making this transition as much of a reset as was the move from Windows Mobile to Windows Phone 7 in 2010. That sounds bad, but the changes coming in Windows Phone 8 should calm some frayed nerves. This is a big release.

Indeed, the feature rundown on Windows Phone 8, even at this early stage—Microsoft didn't reveal many new end-user features at its June Developer Preview event—is long and fairly amazing. It will support multi-core processors and three screen resolutions, 800 × 480 as on existing devices, plus two HD resolutions of 1280 × 720 and

1280 × 768. It will formally support removable and expandable microSD-based storage cards. It will feature always-on device encryption, much like Windows RT, as well as Unified Extensible Firmware Interface (UEFI)–based Secure Boot capabilities.

The new Data Smart feature aims to help users get the most out of their data plans and is based on the metered broadband connection capabilities in Windows 8. It will offer an integrated Skype app that looks and works much like the normal phone experience but also lets third-party apps achieve the same via integrated Rich Communications Suite (RCSe) capabilities. And it will support Near Field Communications (NFC), not just for "tap and share" with other compatible devices, but also for an amazing Microsoft Wallet experience that outdoes both Apple's and Google's similar mobile capabilities.

The Windows Phone 8 camera app is fully extensible via new "lens" apps that take over after the hardware camera button is pressed and enhance camera functionality. New app-to-app communications capabilities will bring a Windows 8–like Share Charm functionality to Windows Phone and will support side-loading of line-of-business apps so that enterprises don't need to go through the Windows Store.

From an end-user perspective, the big new feature is a revised Start screen experience, which does away with the confusing "gutter" of empty space on the right side of the screen, addressing key user complaints. But the big deal is a formalization of the live tile sizes, which will now include three sizes: normal (square), large (rectangular), and the new small size, which is one-quarter the size of normal.

What's interesting here is that every single pinned app or tile can be adjusted by the user to all of these sizes; in Windows Phone 7.x, only Microsoft and wireless carrier tiles could be large. And Nokia's Maps app is coming to Windows Phone 8, benefitting all users and not just those who buy Lumia devices.

There are a ton of other improvements, but I'm running out of space. Be sure to check out my articles "Windows Phone 8 Unveiled" and "Windows Phone Summit" for more information.

Windows Phone 7.8

Windows Phone 8 isn't the only smartphone release that Microsoft will make this year. The software giant is also offering a Windows Phone 7.8 release for existing customers that will provide the single best end-user feature in Windows Phone 8—the new Start screen—to those using current devices.

This won't make everyone happy. I understand why current Windows Phone users are feeling abandoned, but when you consider the engineering headache of porting other features over to a relatively small user base, plus the fact that many of Windows Phone 8's other new features essentially require new hardware, the decision makes sense.

Windows Server 2012 Product Editions

Server 2012 was developed alongside Windows 8, but these products differed in some crucial ways that Microsoft underplayed during the prerelease period. For example, where Windows 8 didn't really hit feature-complete status until its Release Preview (or Release Candidate) phase in mid-year, its Server brother was feature complete back in February at beta. And that means that Server 2012 is actually a bit more mature, if you will, than Windows 8.

But many questions remain. And the big one, for this release, has been what Microsoft intends to do in regard to product editions, or what's still called, anachronistically, SKUs (stock-keeping units—codes identifying products sold in a store).

Windows Server 2008 R2, for example, is a great product line, but like Windows on the client, it's a bit bogged down by a large number of product editions. This includes, but isn't confined to, Windows Server 2008 R2 Datacenter, Enterprise, Standard, Web Server, Foundation, and a version for Itanium-based systems. And let's not forget related products such as Windows Small Business Server 2011 Standard, Windows Small Business Server 2011 Essentials, Windows Home Server 2011, Windows Storage Server 2008 R2 Essentials, and even Hyper-V Server 2008 R2. Whew.

For Server 2012, Microsoft has really gotten the simplification bug. This time around, it offers only four mainstream SKUs: Windows Server 2012 Datacenter, Standard, Essentials, and Foundation.

Datacenter works much like before, with per-processor licensing starting at $4,809, and it features unlimited virtualized instances of the product (on the same hardware). Standard kind of bridges the old Enterprise and Standard SKUs, costs $882 per processor, and provides two virtualized instances of the product (on the same hardware), up from just one in Windows Server 2008 R2 Standard.

Windows Server 2012 Essentials is a direct upgrade to Windows Small Business Server 2011 Essentials, costs $425, and supports small businesses up to 25 users. But Microsoft is finally killing off its legacy Small Business Server Standard product line, which provided on-premises versions of Exchange, SharePoint, WSUS, and, optionally, SQL Server, an unnecessary cost and complexity in this era of cloud computing. Microsoft also killed off Windows Home Server, a beloved but poorly selling product.

The Foundation product is interesting. As with Server 2008 R2, Windows Server 2012 Foundation will be OEM-only, meaning that the only way to acquire it will be with new low-end server hardware. Like Essentials, Foundation lacks Hyper-V, Branch Cache, and some other high-end features, and it targets environments with 15 or fewer users. I'm told that Storage Server will continue forward, but no word yet on an update for Windows Storage Server 2008 R2 Essentials.

Windows 8 Upgrade Pricing

Windows 8 is an amazing leap over its predecessor, but of course many IT pros, admins, and tech enthusiasts are a bit nervous about a new Windows version that bears more resemblance to mobile devices than it does to PC systems of the past. And this nervousness leads to questions about how Microsoft can convince users to upgrade their existing PCs to this new system.

Well, no worries. Microsoft has apparently figured it out.

First, anyone who buys a new Windows 7–based PC between now and February 28, 2013, can get an upgrade version of Windows 8 Pro directly from Microsoft for just $15. At that price, the upgrade is such a no-brainer that even those who are still feeling uncertain about Windows 8 are sure to jump.

Next, and perhaps more interestingly, Microsoft is running a special promotion through which users of existing PCs—running any modern OS from Windows XP and later—can upgrade to Windows 8 Pro for just $40. The promotion starts at the time of Windows 8's general availability and runs through the end of January 2013.

This is a tremendous deal, and one I'd like to see Microsoft make permanent. I suspect Microsoft will find a lot of takers, after people begin perusing new Windows 8–based hardware in the fall—especially those new Surface tablets—and realize they want this system on all their PCs.

I've described this kind of pricing as a "Crazy Eddie" type promotion for good reason. But it's crazy enough to work and, I think, silence the doubters for good. ■

InstantDoc ID 143624

Fine-Tuning Your Active Directory PowerShell Searches

Finding a group/OU intersection

Mark Minasi

is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Email

Twitter

Website

PowerShell's Active Directory (AD)-related search commands (*get-aduser, get-adgroupmember, search-adaccount,* and so on) are some of the things that attracted me most to the new Windows Server 2008 R2 cmdlets, and that's why I've been focusing on them for the past few months. I love the ability to run, for example,

```
get-aduser -f {title -eq "claims adjuster" -and manager
  -eq "cn=JFarkus,cn=users,dc=bigfirm,dc=com"} -searchbase
  "ou=Montana,dc=bigfirm,dc=com"
```

to retrieve all the claims adjusters at Bigfirm.com who are from the Montana OU and who have a manager with the username JFarkus. And that example took me only about 30 seconds to formulate! The hardest part is remembering to use a distinguished name (DN) for a manager—and when I remember how long it took me to do something like that in VBScript, I get a little dizzy.

I'm grateful for the power of the PowerShell cmdlets, but they can be frustrating because, really, they're nothing more than a prettier front end on LDAP queries, and so things that your intuition tells you *should* work—don't (for example, searching to find the people whose managers' names begin with *S*). But when you're using the *get-whatever* AD commands and find yourself in a corner, don't give up: Rather, just try to attack it from a different angle.

And that brings me to last month's puzzle. How do you query AD for a group's members, but to return only the group members who also live in a particular OU? How do you find all the members of the group *folks* who are in the Sales OU?

When I remember how long it took me to do something like this in VBScript, I get a little dizzy.

Maybe you could retrieve a group's membership with *get-aduser* rather than *get-adgroupmember*. You could slap a *-searchbase* parameter on the end, and you'd be in good shape. Whenever I'm up against something like this in PowerShell ("Can *get-something* get a property that will solve the problem?"), I go look at the attributes of the object in question. As you've seen before, you can get an extensive list of the attributes that user objects in PowerShell contain by typing

```
get-aduser -f * | gm
```

By doing that, I see it: MemberOf. Time to take a look at what a typical MemberOf looks like with this command:

```
get-aduser -f {samaccountname -eq "mark"} -pr MemberOf | ft
  name,memberof -auto
```

Recall that *ft* is *format-table* and that if you don't include *-pr MemberOf* in *get-aduser*, you won't get that attribute delivered down the pipeline. MemberOf ends up looking like {CN = Enterprise Admins, CN = Users,DC = Bigfirm,DC = com,CN = Schema Admins,CN = Users, DC = Bigfirm,DC = com . . . } and so on, so essentially MemberOf is a comma-delimited list of the DNs of the various groups that the user named *mark* is a member of.

Next, you'd try using MemberOf in a *get-aduser* filter. Maybe the following query will show us all the people in the Enterprise Admins group?

```
get-aduser -f {MemberOf -like "*Enterprise Admins*"}
```

But unfortunately that returns no results because MemberOf seems to want comparisons with exact DNs of groups. And so

```
get-aduser -f {Memberof -eq "CN=Enterprise Admins,CN=Users,
  DC=Bigfirm,DC=com"}
```

retrieves the members of the Enterprise Admins group, and the only pain it exacts is that you must know the DN of that or any other group. But it's simple to get a list of the groups in a domain and their DNs:

```
get-adgroup -f *|ft name,distinguishedname -auto
```

And from there it's all cut and paste. To return to the original question—"What members of the group *folks* are in the Sales OU?"—you could formulate it like this:

```
get-aduser -f {memberof -eq "CN=Folks,CN=Users,DC=Bigfirm,
  DC=com"} -searchbase "ou=sales,dc=bigfirm,dc=com"
```

Oh, and while we're at it, you could even make that query against a Global Catalog (GC) by adding *-servername:port*, as a member of the AD PowerShell team pointed out to me recently. (Thanks, Saket!) Assuming you want to run the query against a DC named DC4 that was also a GC server, you could run this query:

```
get-aduser -f {memberof -eq "CN=Folks,CN=Users,DC=Bigfirm,
  DC=com"} -searchbase "ou=sales,dc=bigfirm,dc=com" -server
  dc4:3268
```

The morals of this month's story, then, are as follows: It never hurts to give an object's list of attributes another look, and never assume that you should be able to use wildcards against DNs. See you next month! ■

InstantDoc ID 143751

PowerShell Annoyances

Learn to overcome some of PowerShell's confusing features

After leaving Windows PowerShell on the shelf for a few months, I recently had to rework some of my existing scripts for some benchmark tests I was performing for one of our product reviews. I've always been a fan of PowerShell, but in the process of working with these scripts, I couldn't help but notice (i.e., be annoyed by) some of the different PowerShell "features" that are certain to confuse administrators and others who are trying to learn PowerShell. In this column, I'll share the top 10 things that annoy me about PowerShell.

Michael Otey

is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Email

1 Positioning PowerShell as an interactive command console—Maybe it's because I jump in and out of PowerShell according to the tasks I want to accomplish, but I almost never use PowerShell straight from the PowerShell command line. Microsoft uses automation and productivity to sell PowerShell, and you don't get those things by attempting to type in a bunch of complex text commands. You get automation and productivity by running scripts that automate repetitive tasks.

2 Default execution policy prevents scripts from running—I realize this feature is there to secure your scripts, but there's no doubt that just about every PowerShell newbie is going to run into the default Restricted execution policy right out of the gate, which prevents scripts from running. Remember, if you want to run a script, you first need to run *Set-ExecutionPolicy RemoteSigned* or *Set-ExecutionPolicy Unrestricted*.

From the Windows command shell, you can't run a PowerShell script just by entering its name at the command prompt.

3 **Not being able to run PowerShell scripts from the command line**—No wonder Microsoft likes to promote PowerShell as an interactive environment. Even in the PowerShell environment, you can't run a script just by using its name. From the Windows command shell, you can't run a PowerShell script just by entering its name at the command prompt. If you're running a Windows shell, you need to use *powershell -noexit "& "C:\users\mikeo\my script\PSscript.ps1"* to launch a script, which leads directly to my next annoyance.

4 **Calling PowerShell scripts**—It's not enough that you can't start a PowerShell script by typing its name. You can't even easily start it by passing it as a parameter to the powershell.exe executable if the path name has any spaces in it. Instead, you have to add the call operator, &. Adding the & isn't exactly intuitive, and it's definitely a hurdle for beginners.

5 **Not being able to run scripts out of the current directory without an explicit reference**—Another annoyance occurs when you attempt to launch scripts out of the current directory. Unlike the friendlier Windows command shell, PowerShell doesn't load commands from the current directory by default. You must either explicitly supply the path, which is a tedious and error-prone process with today's long path names, or you can use the .\ notation—for example, *".\<script>.ps1"*. If the path name contains blank spaces, you need to enclose it in double quotation marks.

6 **The need to load cmdlets**—The need to load cmdlets is especially a problem in the many PowerShell example scripts that you see for the different server products. The example scripts for different server products won't run until you've loaded the product-specific cmdlets.

7 Cryptic error messages—Cryptic error messages are a problem with almost all software these days, and PowerShell is no exception, with its bright red error messages that you're sure to see frequently when you're new to PowerShell. To reduce these errors, be sure to make use of the PowerShell error-handling statements in your scripts: Trap, Try/Catch/Finally, and Throw.

8 Difficult syntax—Most of PowerShell's syntax is pretty good. Its verb-noun syntax is easy to follow, and prefacing variables with the $ is also easy. However, it's not all so straightforward. For instance, there's the $_, which is often used in loops to represent the current value and can also be used to filter pipeline results. Then when you combine that symbol with brackets and the dot (e.g., {$_. < *name* > }), you've lost most non-developers.

9 Weak Integrated Scripting Environment (ISE)—Yes, PowerShell's ISE is better than Notepad. Yes, it can edit, run, and debug PowerShell scripts. However, it's also the low end of PowerShell development tools. Hopefully, Microsoft will do some work on the ISE with Windows Server 2012, but until then, if you're serious about working with PowerShell, look into PowerWF, PrimalScript, Admin Script Editor, or maybe PowerGUI.

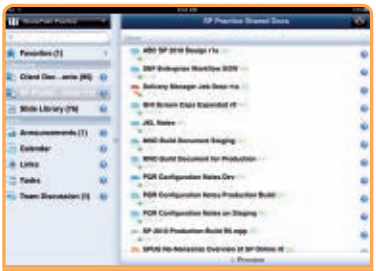
10 Getting Help—For more PowerShell information, start with the built-in PowerShell Help cmdlet. But honestly, reading those text screens isn't easy. For Windows Server 2012, you can check out Windows PowerShell Support for Windows Server 2012. You might also want to watch some of the PowerShell webcasts like, *PowerShell Essentials for the Busy Admin* at Scripting with Windows PowerShell. ■

InstantDoc ID 143534

Colligo Networks

‘Briefcase’ Apps Make SharePoint/iPad Connectivity Easy

The unstoppable business trend of “bring you own device” (BYOD) has been met with varying degrees of enthusiasm by today’s enterprises, as they grapple with how to integrate personal devices within their secure business operations.



▲ Colligo Briefcase Pro View of Document Library

Key instigators of this phenomenon are, without a doubt, the popular Apple iPads, whose ease-of-use and sleek design, coupled with the wealth of business apps now available, have become the business tablet of choice, from the C-suite to the information worker. The challenge begins when organizations seek solutions that enable the productivity gains inherent with mobile devices, while continuing to enforce corporate or regulatory requirements to maintain content in a single, secure repository.

Microsoft SharePoint is another technology enjoying meteoric success over the past several years, selected by tens of thousands of organizations as their collaboration platform of choice. Combining the iPad with SharePoint can result in a powerful, easy-to-use set of tools, but the organization must understand some of the challenges that need to be overcome.

If used “as is,” the iPad’s built-in Safari browser is generally considered to be fairly “clunky” when accessing SharePoint 2010 sites. Fortunately, third-party companies offer productivity-enhancing tools for the iPad, which are often referred to as “briefcase” applications. The basic principle is that the application is downloaded and installed on the iPad and one or more connections are created to the SharePoint site or sites that the user wishes to access. The content of lists and libraries are then synched to the iPad, and the contents of those lists and libraries can then be viewed and, in some cases, edited, whether connected or offline.

All briefcase apps are not created equal, however. When choosing your solution, here are some key features to consider:

▶ **Security.** This is perhaps the most important consideration, and we recommend evaluating apps based on their ability to provide:

- Security features that protect corporate data

in the event that the iPad is lost or stolen. These may include a separate passcode for the briefcase app and/or the ability to wipe content remotely or through iCloud.

- The ability to restrict content access or prevent certain content from being printed, opened in other third-party apps, or shared externally.
- Data encryption; specifically, AES 256-bit hardware encryption, which is highest form available and cannot be disabled by users.
- The inability to back up content to iTunes, so content never leaves the secure confines of SharePoint and the briefcase app.
- The ability to detect and block jailbroken devices (which may inadvertently introduce malware).

▶ **"Smart caching."** This feature enables users to have everything available to them offline or on the road. It has the benefit not only of providing fast access anywhere, but also of reducing a user's wireless roaming charges (if they use a 4G-enabled model) as they can sync on WiFi, and then access all their content offline.

▶ **Ease-of-use.** The best SharePoint apps for iPads meet corporate security requirements, while still providing end users with the intuitive design elements that iPad users know and love, such as touchscreen and swipe. Setup and use should be simple, be it connecting to your SharePoint sites, or navigating from one site or list to another. If your app isn't easy to use, users will find a workaround, opting for unauthorized and unsupported options instead.

▶ **Support for the content that exists in your SharePoint environment.** SharePoint offers a wide range of out-of-the box options, and it's important to test the different "flavors" supported by the app; for example, .msg files, Office documents, PDFs, images, or photos.

▶ **Support for views in SharePoint lists and libraries.** Views are essential to grouping and filtering content in lists and libraries, so your iPad app for SharePoint should support views for both.

▶ **The ability to edit documents as opposed to simply viewing them.** While this typically isn't a capability of the app itself, it should support opening and editing in third-party apps (unless that capability is disabled at the corporate level for security reasons).

▶ **The ability to set storage limits so you don't unwittingly fill up your iPad.**

There are, of course, other issues to consider when allowing SharePoint access on iPads and SharePoint, and evaluating specific apps for use within your organization will be the best way to uncover many of them. However, with the right SharePoint "briefcase" app, you can join the thousands of companies reaping the benefits of SharePoint on iPads today.

▼ Colligo Briefcase Pro Document Properties with Managed Metadata Field Choices

Unleash Your Mobile Workforce

Colligo Briefcase

The simplicity of iPad. The security of SharePoint.

Best of Microsoft TechEd North America 2012

Microsoft Product Awards Featured By: Windows IT Pro | SQL Server Dev Pro | SharePoint Pro

Available on the App Store

- View SharePoint files, including Office documents, PDFs, images and emails
- Edit files, lists and metadata, even while offline
- Sync what you need for easy access
- Easily share files using links to SharePoint documents
- Find content fast with powerful search capabilities
- Collect and transmit data from the field,with advanced support for InfoPath forms

Colligo Networks

www.colligobriefcase.com

Windows Server 2012 Simplifies Active Directory Upgrades and Deployments

What are the fates of Adprep and Dcpromo?

Extending the AD schema to support either a new OS release or Active Directory (AD)-integrated applications that require it (e.g., Exchange Server) is a regular—if infrequent—administrative task. And these kinds of schema upgrades have always made AD administrators nervous. It's not because admins have personal experience with schema upgrades gone bad; if you ask 500 AD admins if they've personally had a bad schema-upgrade experience, 499 of them will admit they haven't. What makes AD admins wary is the fact that upgrading the AD schema can be confusing, and it's irreversible. Anything that affects the entire Windows authentication and authorization infrastructure, and has no "undo" button, is a process to be careful about.

Schema upgrades aren't bothersome only to AD admins; they also irritate Microsoft's Customer Service and Support (CSS) because confusion about the process is a high call generator. Further, adoption of many new AD-related and other features in a new OS was demonstrably slower if the feature depended on a schema upgrade because of the care (and resulting delay) associated with the process. As a result, one of the AD product group's goals for Windows Server 2012 was to make the process simpler, faster, and generally more pain-free than in previous versions. With Server 2012, Adprep has been integrated into the Active Directory Domain Services (AD DS) role installation process.

Adprep is the utility—included in the OS installation media—that performs several crucial functions to upgrade AD to support that

Sean Deuby

is technical director for *Windows IT Pro* and *SQL Server Pro* and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

Email

Twitter

Schema upgrades have always made AD administrators nervous.

OS. The utility has three major options: /forestprep, /domainprep, and /rodcprep. The /forestprep option runs first, extending the AD schema with new object and attribute classes that the new AD version needs. The /domainprep option creates new well-known objects in AD, applies security changes, and enables miscellaneous other bits. Finally, /rodcprep makes forest-wide security changes to allow read-only domain controller (RODC) functionality.

Adprep from Server Manager

The screenshot gallery in my article "Upgrading Active Directory to Windows Server 2012" shows a Windows Server 2008 R2 forest being upgraded to Server 2012 with integrated Adprep and the subsequent promotion of the local DC from Server 2008 R2 to Server 2012. AD admins who didn't pay close attention to the documentation or who didn't read that article will be in for a big surprise, because the Forestprep and domain preparation happens automatically as a result of initiating a Server 2012 DC installation—not beforehand, and with no warning at all. (See image #14 in the screenshot gallery.) This means that if one of your administrators gets the idea to put a Server 2012 DC into a domain, before you know it Adprep will have run its course. So much for careful planning! The other way to view it, of course, is that smaller shops won't have to worry about it.

Adprep from the Command Line

Fear not, you old-school AD admins; you can still run Adprep manually from the \support\adprep folder of the Server 2012 installation disk, if you need to. But a difference from older Adprep versions is that there's no 32-bit version (Adprep32) of the utility. So, you can run Adprep only from a 64-bit version of Server 2008 or later.

You don't have to run Adprep from the schema master, but the Server 2012 server you're running the upgrade from (it doesn't have to be a DC) must have connectivity to the forest's schema master and the domain's infrastructure master. You can now also specify separate

credentials for Adprep /forestprep (Enterprise Admins membership) or /domainprep or /rodcprep (Domain Admins membership) using the /user and /userdomain parameters. This gives you a great degree of flexibility in how you upgrade your forest and domains.

The Death of Dcpromo

Even Dcpromo itself has disappeared. (If you try to run it, a dialog box appears with the text *The Active Directory Domain Services Installation Wizard is relocated in Server Manager*, pointing you to the TechNet article "Installing AD DS by using Server Manager" for information about how to install AD DS.) As the dialog box tells us, the process of installing the AD DS role on a server—thus making it a DC—has been moved to Server Manager. This is more than just a cosmetic move; the AD DS installation process has been completely re-engineered from the ground up. So that it's less susceptible to errors, the process does a number of prerequisite checks before the promotion process ever begins, and either attempts to fix configuration errors or displays a message (in clear language, not developer-ese) describing the failure and suggesting steps to correct it. As with all other administrative tasks in Server 2012, everything you can do in the GUI can be done in PowerShell and vice versa. And you can export a PowerShell script that contains all the options you specified during the GUI installation, so you can reuse it on other DCs in your domain.

Every aspect of the Server 2012 DC installation and AD upgrade process has been examined and redesigned to be as seamless and low-effort as possible. In general, this is a very good thing; just be aware that it's so smooth and seamless that you'll need to guard against an unplanned forest and domain upgrade! ■

InstantDoc ID 143654

Windows IT Pro

SEPTEMBER SCHEDULE OF EVENTS

Web Seminars | In-Person Events | eLearning Events

DevPro SharePoint Pro SQL Server PRO

Web Seminars

All Times Eastern

Wed, Sept.5 @ 2:00 PM
Integrating SharePoint with Exchange: The What's, Why's and How's

Thurs, Sept.6 @ 11:00 AM
Creating Internet-Facing SharePoint Sites with SharePoint 2010

Tues, Sept.11 @ 2:00 PM
What Data Should My Company Place in the Cloud?

Thurs, Sept.13 @ 11:45
Managing Mobile Devices

Mon, Sept.17 @ 12:00 PM
Hours & Dollars: How Idera SharePoint backup Saves You More of Both

Wed, Sept.26 @ 12:00 PM
Looking Ahead: Windows Server 2012 and Virtual Networking Environments with John Savill

eLearning Events

Thurs, Sept.27 @ 11:00 AM
Creating Great User Interfaces

October 2,4,9,11,16,18 @ 11:00 AM
Mastering SharePoint 2010

October 16,23/November 6,13,27/ December 4,11,18 @ 11:00 AM
John Savill Master Series

Don't keep it all to yourself... Send this valuable info to a friend!

New Features of Windows Server 2012 Failover Clustering

Easier management, increased scalability, and greater flexibility

In "Troubleshooting Windows Server 2008 R2 Failover Clusters," I discussed troubleshooting failover clusters—specifically, the locations and tips for where you can go to get the data you need in order to troubleshoot a problem. The Microsoft Program Management Team looked at quite a few of the top problems and worked to improve them in Windows Server 2012 Failover Clustering. So this month, I'll talk about the new features and functionality of Server 2012 Failover Clustering. The new changes for failover clustering offer easier management, increased scalability, and more flexibility.

Scalability Limits

One of the first things to talk about is scalability limits. With Server 2012 clustering, you now have a maximum limit of 64 nodes per cluster. If you're running as a Hyper-V cluster with highly available virtual machines (VMs), the limit has increased to 4,000 VMs per cluster and 1,024 VMs per node.

With these increased limits, Server Manager has been bolstered with the ability to discover and provide remote management capabilities. When you've configured a cluster, it will show all nodes, including the name of the cluster and any VMs on the cluster. In Server Manager, you would see where the remote management can be accomplished, as Figure 1 shows. With this capability, you

John Marlin

is a senior support escalation engineer in Windows Commercial Technical Support, focusing on failover clustering. He has been with Microsoft for over 20 years. He is a Microsoft Certified Trainer for Clustering, delivering to internal Microsoft as well as Microsoft partners, and is a regular contributor to the Ask the Core Team blog.

Email

Blog

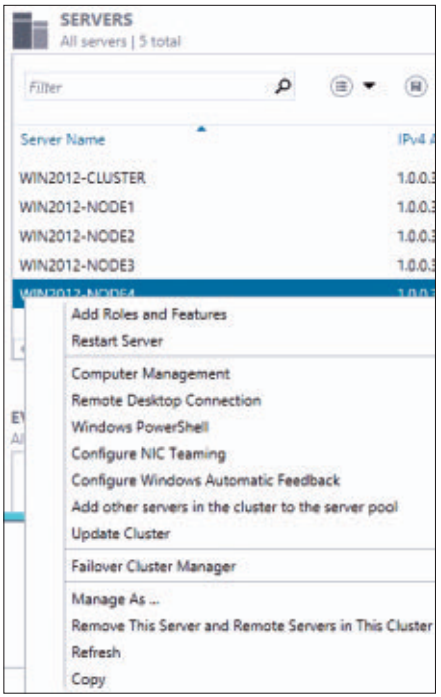


Figure 1
Configuring remote management

can enable additional roles/features remotely.

A New Level of AD Integration

When you're creating a cluster, you'll experience a new level of detection about where the cluster creates an object in Active Directory (AD). When a cluster creates the object, it will detect the organizational unit (OU) where the nodes reside and create the object in the same OU. It will use the logged-on user account to create the Cluster Name Object (CNO), so this account needs to have Read and Create permissions on this OU. If you want to bypass this detection, or place it in a separate OU, you can specify that during the creation. For example, if I want to place the cluster name in an OU called Cluster, during creation I would input the data that Figure 2 shows.

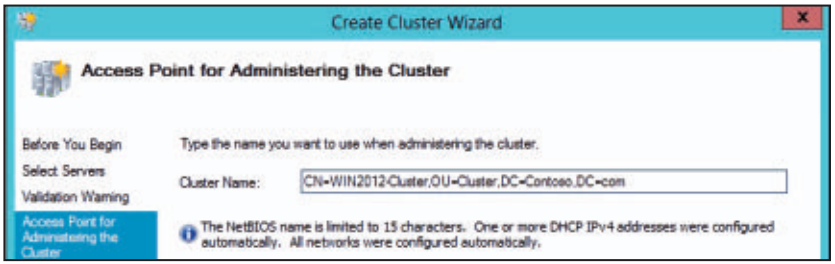


Figure 2
Placing the cluster name in an OU called Cluster

If you're doing it through PowerShell, the command would be

```
New-Cluster "CN=WIN2012-CLUSTER,OU=Cluster,DC=Contoso,DC=com"
  -Node WIN2012-Node1,WIN2012-Node2,WIN2012-Node3,WIN2012-Node4
```

Quorum Configuration

The quorum configuration has been simplified, and a new dynamic quorum model is available—now the default when you're creating a cluster. You can also manually remove nodes from participating in the voting. When you go through the Configure Cluster Quorum Wizard, you're provided with three options:

- *Use typical settings* (recommended)—The cluster determines quorum management options and, if necessary, selects the quorum witness.
- *Add or change the quorum witness*—You can select the quorum witness; the cluster determines quorum management options.
- *Advanced quorum configuration and witness selection*—You determine the quorum management options and the quorum witness.

When you choose the typical settings, the wizard will select the quorum type as dynamic. With a dynamic quorum, the number of votes changes depending on the number of participating nodes. The way it works is that, to keep a cluster up, you must have a *quorum* or *consensus* of votes. Each node that participates in a cluster is a vote. If you have also chosen to have a witness disk or share, that's an additional vote. To keep the cluster going, more than half of the votes must continue to run. You can use the math equation of (total votes + 1)/2. I have nine total nodes in a cluster without a witness disk. So, using the math equation above, it would be (9 + 1)/2 or 5 total votes to keep the cluster up.

So, for example, consider what occurs with a Server 2008 R2 cluster and a Server 2012 cluster. In a Server 2008 R2 cluster, using the same nine nodes in the cluster, this means that I have nine total votes and will need five votes (nodes) to remain going to keep the cluster up. If there are only four nodes up, the cluster service will terminate because there aren't enough remaining votes. The administrator would need to take manual actions to force the cluster to start and get back to production. In a new Server 2012 failover cluster, when a node goes down, the number

of votes needed to remain up also dynamically goes down. With my nine nodes (votes), if one node (vote) goes down, the total vote count becomes eight. If another two nodes go down, the vote count becomes six. The Server 2012 cluster will continue running and stay in production without intervention needed. Dynamic Quorum is the default and recommended quorum configuration for Server 2012 clusters.

To change the quorum witness configuration, you can right-click the name of the cluster in the far left pane, choose More Actions, and select Configure Cluster Quorum Settings, as Figure 3 shows. The wizard will let you set a disk witness, set a file share witness, or leave it as dynamic. If you choose the advanced settings, one of the first settings you'll determine is what nodes actually have a vote in the cluster, as Figure 4 shows. All nodes participate with a vote to achieve quorum. If you de-select a node, it won't have a vote. Using the earlier example of nine nodes, for Server 2008 R2 clusters, you have only eight voting

Figure 3
Changing the quorum configuration

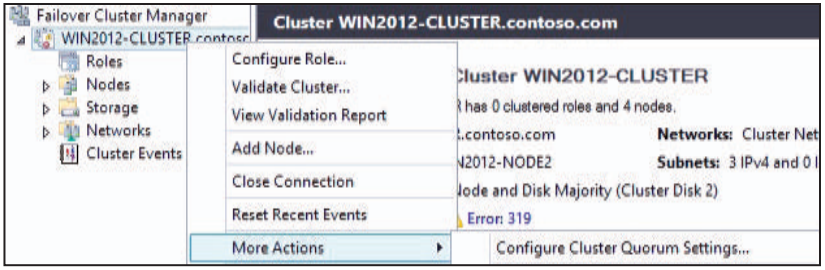
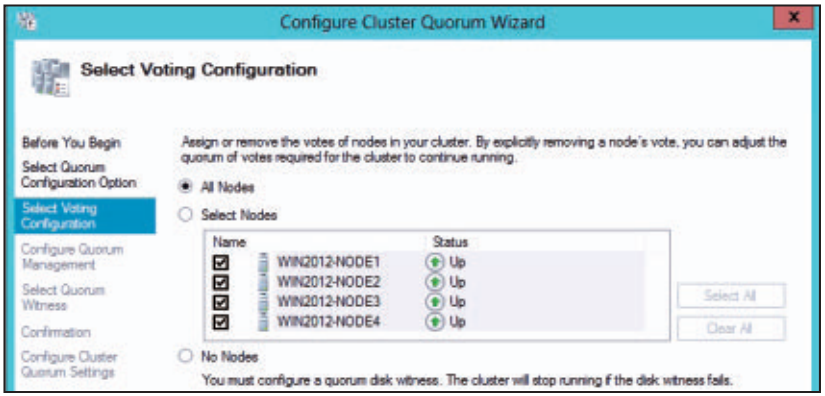


Figure 4
Determining which cluster nodes have a vote



members, so a witness disk or share would need to be added. In both Server 2008 R2 and Server 2012 clusters, this non-voting node doesn't have a vote; if it's the only node left, the cluster service will stop and manual intervention will be necessary.

When going through the Configure Cluster Quorum Wizard, the next screen shows the option where you can select or de-select the dynamic quorum option, as Figure 5 shows. As you can see, the default action is selected and is also recommended. If you want to change the quorum configuration to add a witness disk or share, the next screen in the wizard, Select Quorum Witness, is where you can choose the witness disk or share to use.

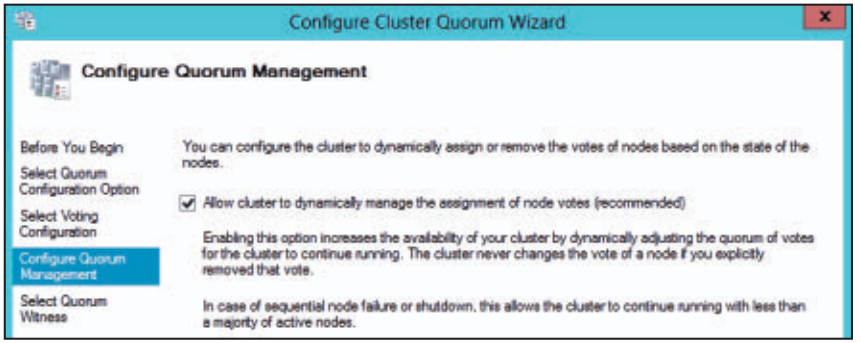


Figure 5
The Configure Quorum Management page

Cluster Validation

There are some new cluster-validation enhancements. One of the big benefits is that storage tests will run significantly faster. The storage tests measure things such as which node can see the drives, determine failovers individually and as groups to all nodes, check to see if the drive can be yanked away from each node from the other nodes, and so on. In Server 2008 R2 failover clusters, if you had a large number of disks, the storage tests took a lot of time to complete. With Server 2012 cluster validation, the tests have been streamlined in their execution and in the speed they take to complete. A new option for the storage tests is that you can target specific LUNs to run the tests against, as you can see in Figure 6. If you

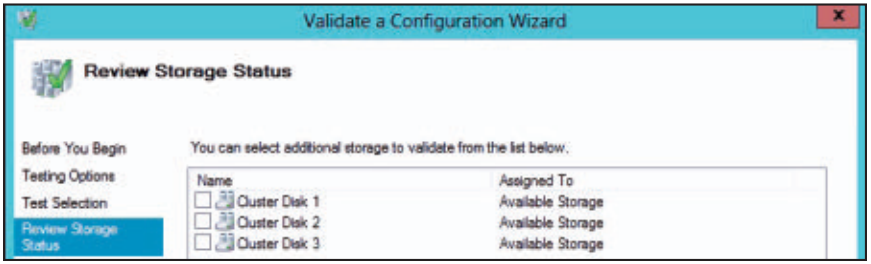


Figure 6
Reviewing your storage status

want to test a single LUN or a specific set of LUNs, just select the ones you want.

There are also new tests for Cluster Shared Volumes (CSV) as well as for Hyper-V and the VMs. These tests check to see if your networking is configured with the recommended settings to ensure that network connectivity can be made between machines, quick/live migrations are set up to work, the same network switches are created on all nodes, and so on.

Cluster Virtual Machine Monitoring

When you're running highly available VMs with the Hyper-V role in a cluster, you can take advantage of a new feature called Virtual Machine Monitoring. With this new monitoring, you can actually have Failover Clustering monitor specific services within the VM and react if there is a problem with a service. For example, if you're running a VM that provides print services, you can monitor the Print Spooler service. To set this up, you can:

1. Right-click the VM in Failover Clustering.
2. Choose More Actions.
3. Choose Configure Monitoring.
4. Choose the service or services that you would like to monitor.

If you want to set this up with PowerShell, the command would be

```
Add-ClusterVMMonitoredItem –VirtualMachine "VM Name" –Service
  Spooler
```

Failover Clustering will then "monitor" the VM and service through periodic health checks. If it determines that the monitored service is unhealthy, it will consider it to be in a critical state. It will first log the following event on the host. For example:

```
Event ID: 1250
Source: FailoverClustering
Description: Cluster Resource "Virtual Machine Name" in
  clustered role "Virtual Machine Name" has received a critical
  state notification. For a virtual machine this indicates that
  an application or service inside the virtual machine is in an
  unhealthy state. Verify the functionality of the service or
  application being monitored within the virtual machine.
```

It will then restart the VM (forced shutdown, but graceful) on the host that it's currently running on. If it fails again, it will move it to another node to start. Virtual Machine Monitoring gives you a finer granularity of the kind of monitoring you want to have for your VMs. It also brings the added benefit of additional health-checking, as well as availability. Without Virtual Machine Monitoring, if a particular service has a problem, it would continue in that state and user intervention would be required to get it back up.

Cluster Aware Updating

Cluster Aware Updating (CAU) is new to Server 2012 Failover Clustering. This feature automates software updating (security patches) while maintaining availability. CAU offers the following actions:

- Apply updates to this cluster
- Preview updates to this cluster
- Create or modify the Updating Run Profile
- Generate a report on past Updating Runs
- Configure cluster self-updating options
- Analyze cluster updating readiness

CAU will work in conjunction with your existing Windows Update Agent (WUA) and Windows Server Update Services (WSUS) infrastructures to apply important Microsoft updates. When CAU begins to update, it will go through the following steps:

1. Put each node of the cluster into node maintenance mode.
2. Move the clustered roles off the node. In the case of highly available VMs, it will perform a live migration of the VMs.
3. Install updates and any dependent updates.
4. Perform a reboot of the node, if necessary.
5. Bring the node out of maintenance mode.
6. Restore the clustered roles on the node.
7. Move to update the next node.

You can start CAU from Server Manager, Failover Cluster Manager, or a remote machine. The recommendations and considerations for setting this up are as follows:

- Don't configure the nodes for automatic updating either from Windows Update or a WSUS server.
- All cluster nodes should be configured to use the same update source (WSUS server, Windows Update, or Microsoft Update).
- If you update using Microsoft System Center Configuration Manager 2007 and Microsoft System Center Virtual Machine Manager 2008, exclude cluster nodes from all required or automatic updates.
- If you use internal software distribution servers (e.g., WSUS servers) to contain and deploy the updates, ensure that those servers correctly identify the approved updates for the cluster nodes.
- Review preferred owner settings for clustered roles. Configure these settings so that after the software-update process, the clustered roles will be distributed across the cluster nodes.

Alternative Connections

In the previous versions, the only way you could connect to a share is with the Client Access Point (the network name in the group)

because the shares were *scoped* to only this name. More information about this behavior is explained in the blog post "File Share 'Scoping' in Windows Server 2008 Failover Clusters." This limited the way administrators had clients connect to shares because there was only one option to connect. This was a big problem with administrators because, in some cases, it made server consolidations more difficult and time consuming because additional steps needed to be taken into consideration—which, in turn, led to longer downtimes to perform the consolidations. Because of this, Server 2012 Failover Clustering now gives you the ability to connect to shares via the virtual network name, the virtual IP address, or a CNAME that is created in DNS. One caveat is that when using CNAMEs, additional configuration is needed for the name. For example, suppose you had a file share with the clustered network name TXFILESERVER and you wanted to set up a CNAME of TEXAS in DNS to connect. Through PowerShell, you would execute

```
Get-ClusterResource "TXFILESERVER" | Set-ClusterParameter
  Aliases TEXAS
```

When this is done, you must take the name offline and put it back online before it will take effect and answer the connection.

You need to consider the repercussions of connecting via the IP address or alias. When connecting via these methods, Kerberos won't be the authentication method used because it will drop to using NTLM security. So, although connecting via these alternative methods does bring flexibility, the security trade-off for NTLM authentication must be taken into consideration.

CSV Updates

CSV has been updated with the following list of capabilities. These features provide for easier setups, broader workloads, and enhanced security and performance in a wider variety of deployments.

- Storage capabilities for Scale-Out File Servers (more on this later), not just highly available VMs
- A new CSV Proxy File System (CSVFS) to provide a single, consistent filename space
- Support for BitLocker drive encryption
- Direct I/O for file data access, enhancing VM creation and copy performance
- Removal of external authentication dependencies when a domain controller (DC) might not be available
- Integration with Server Message Block (SMB) 3.0 to provide for file servers, Hyper-V VMs, and applications such as SQL Server
- Use of SMB Multichannel and SMB Direct to allow CSV traffic to stream across multiple networks, and use of network adapters that support Remote Direct Memory Access (RDMA)
- Ability to scan and correct volumes with zero offline time as NTFS identifies, logs, and repairs issues without affecting the availability of CSV drives

Scale-Out File Servers

Scale-Out File Servers can host continuously available and scalable storage, by using the SMB 3.0 protocol, and utilizes CSV for the storage. Benefits of Scale-Out File Servers include the following:

- Provides for active-active file shares in which all nodes accept and serve SMB client requests. This functionality provides for transparent failover to other cluster nodes during planned maintenance and unplanned failures.
- Increases the total bandwidth of all file server nodes. There's no longer the bandwidth concern of all network client connections going to a single node; instead, a Scale-Out File Server lets you transparently move a client connection to another node to continue servicing that client without any network disruption. The limit to a Scale-Out File Server at this time is eight nodes.

- CSV takes the improved Chkdsk times a step further by eliminating the offline phase. With CSVFS, you can run Chkdsk without affecting applications.
- Another new CSV feature is CSV Cache, which can improve performance in some scenarios such as Virtual Desktop Infrastructure (VDI).

Scale-Out File Servers are ideal for SQL Server and Hyper-V configurations. The design behind Scale-Out File Servers is for applications that keep files open for long periods of time, as do most data operations. A SQL Server database or a Hyper-V VM .vhd file performs a lot of data operations (changes to the file itself), but doesn't perform a lot of actual metadata updates. It shouldn't be used as a user data share where the workload has a high number of NTFS metadata updates. With NTFS, metadata updates are operations such as opening/closing files, creating new files, renaming existing files, deleting files, and so on that make changes to the file system of the drive.

Always Improving

Our Microsoft Program Management Team has worked hard and listened to users about features they've been wanting from failover clusters, and the team has delivered. We've also taken some of the top issues seen in previous versions and made them into positives with the new version. ■

InstantDoc ID 143764

Reader to Reader

Apostolos Fotakelis

is a computer security engineer, a CISSP, and a Microsoft Certified Trainer. He has a bachelor's degree in mathematics.

Email

Website

10 Free Security Tools for Home Use

Nowadays, security needs to be the #1 priority on Windows PCs, even those used at home. Here are 10 free tools you can use to increase the level of security on your home PCs.

Windows Firewall, Windows Update, User Account Control

Although Windows Firewall, Windows Update, and User Account Control (UAC) are built into many versions of Windows, I'm amazed by the number of PCs that have these three tools turned off. Also amazing is that some people pay for utilities that replicate what Windows Firewall and Windows Update do for free. In short, Windows Firewall helps you protect your computer by blocking unauthorized network connections. Windows Update ensures that your OS and Microsoft applications are updated with all the latest patches. UAC (in Windows Vista and later) helps distinguish between authorized and non-authorized changes or actions in your computer. For more information about these tools, see the Security & Safety web page.

Microsoft Security Essentials

Microsoft Security Essentials is not only free but also uses few resources. It guards against viruses, spyware, and other malware. An extra advantage is its "low-profile" approach to security: It notifies you only when it's really necessary.

McAfee SiteAdvisor

The McAfee SiteAdvisor browser plug-in makes it easy for you to identify the reputation of a website before you click the link. It's ideal when a page contains multiple links (such as a search engine's result

page) and you aren't sure which one to trust. There's also a paid version that provides additional security features.

Secunia Personal Software Inspector

Secunia Personal Software Inspector will scan your disks and detect most (if not all) instances of outdated programs, DLLs, and ActiveX components, including Adobe Flash Player, Java, and Adobe Shockwave Player. In most cases, it will give you the option to automatically update them. I can't stress its usefulness enough!

Windows Virtual PC

Windows Virtual PC or another virtualization product can be an invaluable security tool when you need to run programs or visit websites you don't trust. In addition, you can use a virtualization product to create dedicated virtual machines (VMs) with minimal software installed on them just for connecting to sensitive sites, such as the site you use for online banking.

Enhanced Mitigation Experience Toolkit

Microsoft's Enhanced Mitigation Experience Toolkit (EMET) is a commonly misunderstood tool, even by its supporters. It can provide an additional layer of protection that can be useful for applications that are common targets for zero-day exploits, such as Microsoft Internet Explorer (IE), Adobe Reader, Adobe Flash Player, and Java. More and more of the technologies EMET leverages are finding their way to newer Windows versions, which makes EMET a useful tool especially for older OSs, such as Windows XP. Its latest version (EMET 3.0) also exposes some new features (such as configuration through a Group Policy Object—GPO) that bring it a step closer to enterprise deployment.

Sandboxie

Sandboxie offers the capability to run a program in a sandbox when there's need to do so or even permanently. This means that the

EMET can provide an additional layer of protection that can be useful for applications that are common targets for zero-day exploits.

damage will be contained if the program gets compromised. It's useful when browsing less-trusted websites or opening untrusted documents, which makes Adobe Acrobat, Microsoft Office, and IE good candidates. The concept is similar to virtualization but Sandboxie is much less resource intensive and much more convenient, although not as powerful. Personal use of Sandboxie is permitted free of charge for as long as you want. There's also a paid version that removes the nag screen of the free version and provides some additional features you might appreciate.

VirusTotal

VirusTotal is a website that you can use when you're suspicious about the malicious nature of a file or URL. After you upload the file or provide the URL, this free service will check it against more than 40 different anti-malware products and present you with the results.

Create Your Own Line of Defense

Some of these tools can be repurposed and still stay within the "stay secure" concept. For example, Sandboxie can be used as an alternative to IE's InPrivate Browsing mode. However, none of the tools can be totally replaced by another. So, you should mix and match to create your own line of defense. ■

InstantDoc ID 143482

FAQ

Answers to Your Questions

Q: How do I perform a migration from Windows Server 2008 R2 Hyper-V failover clusters to Windows Server 2012 Hyper-V failover clusters, with no downtime?

Jan De Clercq

A: For some time now, the Windows Failover Clustering feature hasn't let you do a rolling upgrade with a mix of OSs in a single cluster. This is due to radical differences and improvements with each new version of Failover Clustering. When you add to that the major changes in Hyper-V between Windows Server 2008 R2 and Windows Server 2012, it becomes clear that a mix of server versions in a single cluster won't be possible.

What will be provided is a migration wizard, which should help make the migration of turned-off virtual machines (VMs) from the Server 2008 R2 cluster to the Server 2012 cluster fast and simple. However, because the VMs need to be turned off during migration, you need to budget for a small amount of downtime in your migration plan.

—John Savill

InstantDoc ID 143146

William Lefkovics

Q: Can I turn off UAC to get rid of all the UAC prompting dialog boxes?

John Savill

A: Yes, you can turn off User Account Control (UAC), but I don't recommend it because it weakens the overall security posture of your Windows system by giving more opportunities for malware to get installed and do harm on your system.

To turn UAC off in Windows 7, type UAC in the Start menu search box to bring up a link called Change User Account Control Settings. Click this link to open the User Account Control Settings dialog box, then drag the slider all the way down to the bottom to disable UAC entirely—as Figure 1 shows.

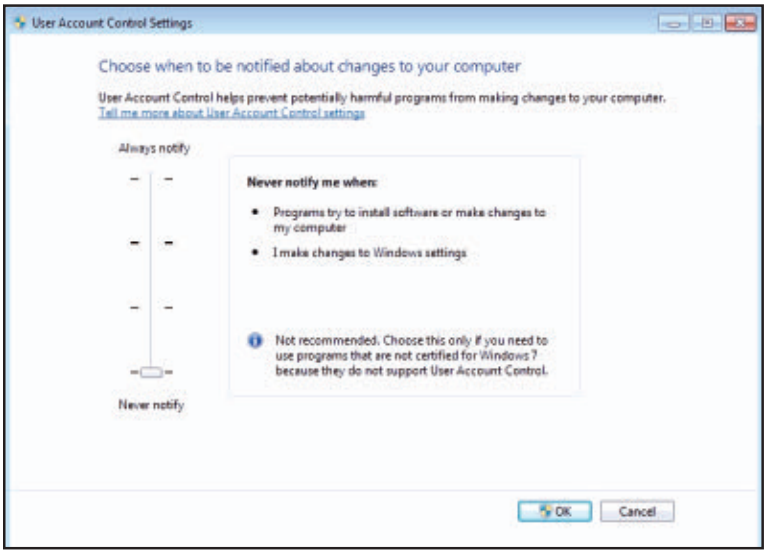


Figure 1
Turning off UAC in the User Account Control Settings dialog box

To turn UAC off in Windows Vista, type UAC in the Start menu search box to bring up the link *Turn User Account Control (UAC) On or Off*. Click this link; then, on the resulting screen, clear the check box for Use User Account Control (UAC). Click OK. For both Windows 7 and Vista, you'll need to reboot your system before the changes take effect.

Microsoft also provides Group Policy Object (GPO) settings to let administrators change and fine-tune the default UAC prompt behavior for limited-account and privileged-account users. You can find the UAC-related GPO configuration settings, which start with the words User Account Control, in the \Security Settings\Local Policies\Security Options GPO container.

—Jan De Clercq

InstantDoc ID 143466

Q: What are my certification options for Microsoft Outlook?

A: Perhaps you have users looking to add to their resume or standing within the company. Or maybe you want to know what to look for when hiring users who claim to hold Outlook certifications. Microsoft maintains a certification path for Microsoft Office applications called Microsoft Office Specialist. The MOS certification is attained through the completion of one or more of the Microsoft-created exams that test the Microsoft Office applications, including Outlook. Microsoft exams are offered through various authorized testing centers around the world. A specific exam tests Microsoft Outlook: Exam 77-884. This exam is generally more for users of Microsoft Outlook 2010; it doesn't cover aspects of installation, corporate deployment, or optimizing Outlook for use with Microsoft Exchange Server.

Exam 77-884: Outlook 2010 tests everyday use of Outlook as well as configuration of the working environment, which includes the various settings in the Office Backstage view, found under File, Options in Outlook 2010. The exam challenges the user in managing the various Outlook items, from email messages and contacts to tasks and calendar items. Users need to know how to manipulate Outlook's message hygiene features, including junk email settings and Outlook rules.

Third-party companies, such as National Computer Science Academy, offer their own certifications in Office applications, including Outlook. However, to use the official Microsoft Office Specialist certification title for Outlook 2010, you must have completed Exam 77-884: Outlook 2010. Third-party exams don't grant you a Microsoft certification. For more information about Microsoft certifications, peruse the Microsoft Learning website.

—William Lefkovics

InstantDoc ID 143508

Q: Is there an updated spreadsheet that contains all Group Policy settings, including Windows 8?

A: Windows 8 Group Policy settings and corresponding registry values can be found in a Microsoft Excel spreadsheet maintained by Microsoft. This spreadsheet contains every Group Policy setting and its corresponding registry value (where appropriate), including those for Windows 8. You can download the spreadhseet at the Microsoft download site. You'll find many settings specific to Windows 8 and Internet Explorer (IE) 10 that focus on new features.

—John Savill

InstantDoc ID 143255

Q: Is there an easy way to convert a VMware virtual machine or template to a Hyper-V virtual machine?

A: Several virtual-to-virtual (V2V) solutions enable conversion of VMware virtual machines (VMs) and templates to Hyper-V format. System Center Virtual Machine Manager includes this capability.

Microsoft has released a new conversion tool, currently in beta and available from the Microsoft site. It's called the Microsoft Virtual Machine Converter Solution Accelerator. It converts VMs created on VMware vSphere 4.1 or 5.0 running guest OSs Windows Server 2003 SP2, Windows Server 2003 R2 SP2, Windows Server 2008 R2, or Windows 7 to a Windows Server 2008 R2 SP1 Hyper-V VM.

The tool converts the virtual hard disks (VHDs) from VMware, and the CPU, memory, and other configuration settings, but not the network adapter configuration. The tool can also be used just to convert hard disk files, and a command-line utility, MVMC.EXE, is provided to enable command-line or scripting conversions.

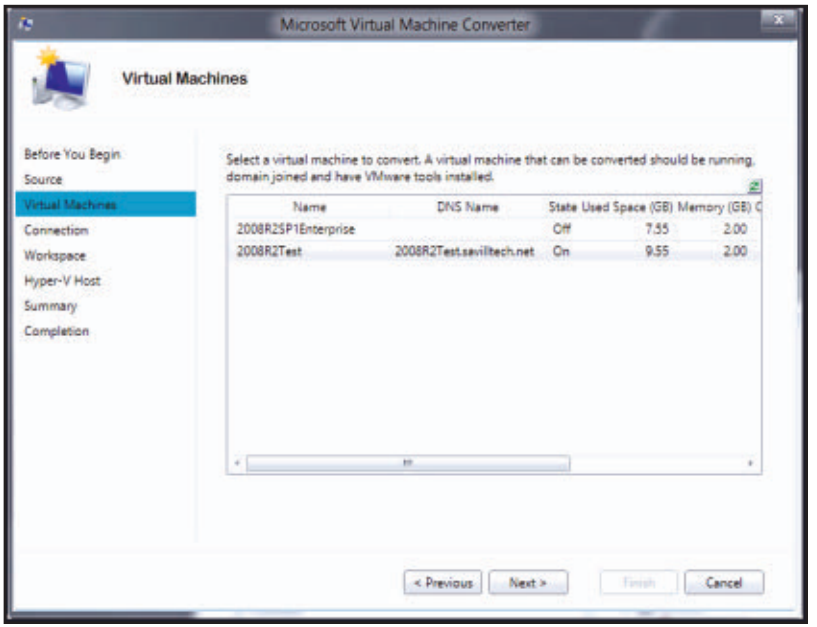


Figure 2
UI for Microsoft Virtual Machine Converter

The graphical wizard lets you select a VMware ESX Server or vCenter Server, and any supported VM that's domain-joined can be selected and converted after you choose a temporary path for the conversion and the final Hyper-V host (see Figure 2).

—John Savill

InstantDoc ID 143302

Q: When I run Windows PowerShell Invoke-Command on more than 32 remote servers, the command runs only on the first 32 servers and queues the others. How can I change this?

A: The queuing of commands is by design, done to control the number of concurrent remote command executions. However, you can change the concurrent limit by using the -ThrottleLimit <value> parameter for Invoke-Command to increase it. Here's an example of how to use it:

```
Invoke-Command -ThrottleLimit 64
  -ComputerName a,b,c -ScriptBlock {command}
```

where {*command*} contains the actual commands you want to run on all the remote servers.

—John Savill

InstantDoc ID 143142

Q: Is there an easy way to integrate Twitter with Microsoft Outlook 2010?

A: Many of us depend on Outlook as our personal information manager (PIM), well beyond simple email. Meanwhile, Twitter has continued its impressive growth both on personal and business levels. Nearly three years ago, I wrote about a third-party Outlook add-in called TwInbox that brought Twitter into your Outlook 2007 client. Now TwInbox also works well in Outlook 2010.

Twitter often updates its API, so Twitter clients are sometimes left scrambling to adjust to any changes. TwInbox has continued supporting its Outlook add-in, and the product continues to provide excellent Outlook integration with Outlook 2010. TwInbox is still a 32-bit application, but it works well on both 32-bit and 64-bit Outlook installations.

Like most Outlook add-ins, Outlook should be closed prior to installation. After TwInbox is installed, it loads with Outlook at the next restart. TwInbox is added to the Ribbon on both the Home tab, which Figure 3 shows, and the Add-Ins tab.

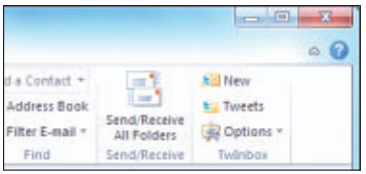


Figure 3
TwInbox options on the Outlook 2010 Ribbon

Obviously, before TwInbox can pull and render your Twitter timeline, you have to configure it to do so. From the TwInbox pane of the Home tab of the Ribbon, select Options, Options to launch the TwInbox configuration wizard. However, the wizard appears only if no accounts have been set up yet. The wizard prompts you to sign in to Twitter with

a standard OAuth request using your Twitter username and password. Next, you choose a folder where tweets will be stored.

After your Twitter account has been verified, you're ready to tweet. Figure 4 shows the folder hierarchy for TwInbox within the folder selected in the configuration wizard. It also shows the dialog box that opens when you select RT with a tweet highlighted in Outlook.

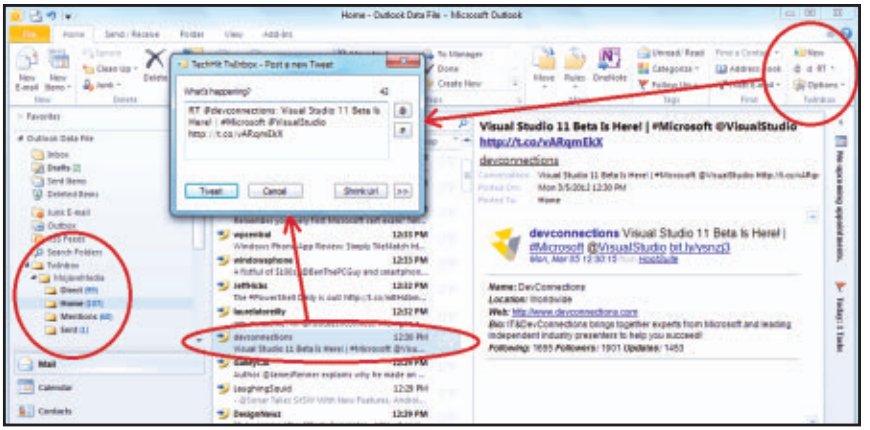


Figure 4
Using TwInbox in Outlook 2010

All the standard tweet options are available from the main Outlook interface, including direct messages (DM), retweets (RT) and favorites. When you upload an image, TwInbox offers the choice of three image hosting services (independent of TwInbox and Twitter). TwInbox also employs bit.ly as a URL shortener to help users meet the 140-character limit.

In a corporate environment, you might have designated tweeters for specific Twitter accounts, or you might have an individual responsible for multiple Twitter accounts. TwInbox allows multiple Twitter accounts through the Outlook add-in.

By default, a new parent folder for each account is created under the folder you selected in the configuration wizard. Additional accounts and preferences are set up from the Options button in the TwInbox pane of the Ribbon. You can set preferences that affect TwInbox as a whole and preferences specific to each Twitter account. When you

have multiple Twitter accounts configured, you select an account from a drop-down menu when you compose a new tweet to determine which account the tweet is sent from.

If you're following a lot of people on Twitter, I recommend not using the TwInbox account option to create individual folders for each sender. This option creates individual subfolders as each unique account in your timeline sends tweets. If you follow thousands of people or accounts, it could result in thousands of separate folders in Outlook. Using Outlook as a Twitter client, however, allows offline searches of your timeline indexed within Outlook. You can also easily archive tweets you send when you configure TwInbox to save messages you send. This setting isn't the default, but you configure it in Account Settings by simply selecting the check box.

A couple of features aren't configurable when TwInbox is installed on Outlook 2010. TwInbox displays the most recent inbound tweets in the Add-Ins tab in Outlook 2010, which Figure 5 shows. In Outlook 2007, there were options to have buttons in the toolbar to launch the Tweet dialog box. With the more complete Ribbon in Outlook 2010, this option is no longer available.

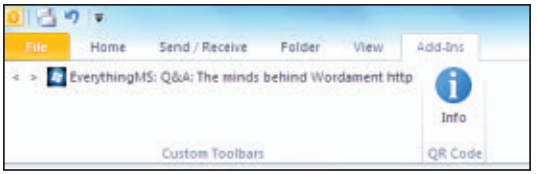


Figure 5
TwInbox showing the latest inbound tweet in the Add-Ins tab in Outlook 2010

If maintaining social media accounts is your entire job, TwInbox might not be the best tool for Twitter, considering the available dedicated desktop clients, such as TweetDeck, HootSuite, and Seesmic. However, if you're trying to maintain Outlook as your sole dashboard for communication, TwInbox can handily provide the Twitter client component. ■

—William Lefkovics

InstantDoc ID 143620

Exchange Server 2013 Preview

A whole new version of Exchange, three years in the making

A new star has appeared on the horizon: Microsoft announced the preview edition of Exchange Server 2013 on July 16 along with the other servers and clients that collectively form the Office 2013 "wave." Exchange 2013 represents three years of output from a large engineering group and includes numerous changes, improvements, and tweaks that I could discuss; however, I don't have the space to cover everything. Instead, let's concentrate on the features that might convince CIOs to approve an upgrade. Understanding the value that the new features provide will help you decide whether and when to upgrade your environment. Keep in mind that Microsoft is still working on Exchange 2013, and some details might change between the preview edition discussed here and general availability.

Deployment Basics

As in Exchange 2010 and Exchange Server 2007, Microsoft doesn't support in-place upgrades for Exchange 2013. Instead, you must deploy on new or reused hardware. Because of a change in the way that Client Access servers process user credentials to comply with a

Tony Redmond

is a senior contributing editor for *Windows IT Pro* and the author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press).

Email

Twitter

Blog

Exchange 2013 represents three years of output and includes numerous changes, improvements, and tweaks.

new "serialized common security context" and the need to update Exchange 2010 with new code to interoperate with Exchange 2013, you must upgrade your Exchange 2010 servers to Service Pack 3 (SP3), which isn't scheduled for release until early 2013. You also must install an Active Directory (AD) schema update to prepare the way for new functionality such as "modern" public folders (which I discuss later). If you're still running Exchange 2007, you need to update those servers with a patch that Microsoft has yet to finalize. Exchange 2003 servers are no longer supported in an organization after you upgrade to Exchange 2013.

Exchange 2013 supports Windows Server 2008 R2 (SP1 or later) or Windows Server 2012. Although components such as PowerShell 3.0 are exploited, it's not yet clear whether Exchange 2013 will take advantage of some of the advanced new features of Server 2012. For example, database availability groups (DAGs) use Windows failover clustering, which supports up to 64 servers on Server 2012. It would be nice if Exchange 2013 supported more than the current 16-server limit in a DAG. Every AD site into which you deploy Exchange 2013 must have at least one Server 2008 (or higher) Global Catalog (GC) and domain controller (DC), and the overall forest must be at Windows Server 2003 functional level or higher. Exchange 2013 doesn't support read-only DCs (or GCs), nor is it possible to run Exchange 2013 on Server 2012 Server Core.

When you install Exchange 2013, you'll see that server roles have been simplified. We now have Client Access servers and Mailbox servers, both of which are different from their Exchange 2010 or Exchange 2007 equivalents, and both of which have taken over some aspects of the work previously done by Hub Transport servers. Client Access servers are designed to be stateless servers that proxy incoming connections from all protocols, including SMTP. Unlike older Client Access servers, Exchange 2013 Client Access servers support TCP (layer 4) affinity to make load balancing easier. By comparison, Exchange 2010 and Exchange 2007 load balancing is based on layer 7 affinity, so if you use hardware load balancers, you need to check with your vendor

to establish whether changes are required to support Exchange 2013. The upshot is that these changes dramatically reduce the complexity of load balancing in an Exchange environment.

Although they appear similar to their predecessors, Exchange 2013 Mailbox servers represent a major evolution of the Exchange 2010 model. All rendering and other processing of messages occurs on Mailbox servers. (Client Access servers perform some of this work in Exchange 2010.) This simplifies processing if a failure occurs because everything switches to the Mailbox server that activates the failed databases. Client Access servers now focus solely on making sure that client connections get to the correct Mailbox servejr.

Communication between Client Access servers and Mailbox servers is through either HTTP (MAPI RPCs are wrapped in HTTP) for client traffic or SMTP for transport. Exchange 2013 doesn't yet have an Edge Transport server role, but you can continue to use Exchange 2010 (SP3) Edge servers until Microsoft updates these servers.

Microsoft recommends upgrading Internet-facing sites first, followed by internal sites. This approach allows Exchange 2013 Client Access servers to take over the organization's namespace and support incoming connections for both down-level Exchange 2010 and Exchange 2013 servers. Microsoft also recommends that you either install both roles on the first Exchange 2013 server installed or make sure that at least one server of each type is deployed. PowerShell cmdlets are executed only on Mailbox servers, so you need to have an Exchange 2013 Mailbox server available to be able to manage the environment.

Microsoft's goal is that you should be able to update Client Access servers and Mailbox servers independently. In the future, it should be possible to mix and match Client Access servers and Mailbox servers running different software versions without any problems. Splitting Exchange into thin protocol servers and thick compute engines addresses some of the current complexity, in which all of the Exchange components that interact with a user's mailbox must be upgraded together. The new architecture also delivers a useful benefit for Office

365 because Exchange 2013 will be much easier for Microsoft to deploy and update in its data centers than its predecessors are.

Database Updates

Exchange 2013 continues to use the Extensible Storage Engine (ESE) for its databases, which are populated by moving mailboxes from Exchange 2010 or Exchange 2007 servers. You can't move mailboxes directly from Exchange 2003 servers; these moves must go through an intermediate Exchange 2010 or Exchange 2007 server.

For the third version in succession, Microsoft's Exchange engineers have focused on the efficiency of the Exchange Information Store. All Exchange 2010 and Exchange 2007 Store code has been rewritten in new managed code modules, resulting in a further reduction in the I/O footprint per active mailbox. More memory is used to cache data to avoid expensive disk I/O.

Microsoft learned a lot from Exchange 2010 customer deployments, as well as from the company's own experience running Exchange Online for millions of mailboxes. Multiple disk failures in JBOD arrays (approximately 5 percent for 7.2K rpm SATA drives and 2.75 percent for 7.2K rpm SAS disks) resulted in the frequent need to reseed database copies on replaced disks. Because reseeding operations from a single source is slow, Exchange 2013 can now reseed a database copy from all available copies. According to Microsoft, it's now possible to complete a reseed operation for a 2TB database in approximately 10 hours rather than the 23 hours previously required if three healthy database copies are available. Although not many installations operate 2TB+ databases, I appreciate the fact that operational experience from Office 365 is driving improvements that benefit on-premises customers.

Because of a change in the way mailbox properties and other overhead are more accurately included in the calculation of mailbox size, you can expect to see mailbox sizes grow by approximately 30 percent. No increase in physical database size occurs, but you might

have to adjust some assigned mailbox quotas to accommodate the new overhead.

Exchange 2013 updates the Transport Dumpster feature to better support lagged database copies. A lagged database copy is designed to remain a predefined time period (up to 7 days) behind the live database copy and is intended to provide a backup for database recovery in case a problem occurs that corrupts the live database and its other copies. Exchange 2013 expands the Transport Dumpster feature so that the Transport Dumpster understands when a server supports lagged copies and therefore keeps copies of messages until they're committed into the lagged copy. This change is small but important.

A New Era of Administration

A central theme in Server 2012 is remote administration. Exchange 2010 demonstrates the effectiveness of this approach by using remote PowerShell as the underlying foundation for all of its management interfaces, including the Microsoft Management Console (MMC)–based Exchange Management Console (EMC).

Exchange 2010 added a browser-based administration console, the Exchange Control Panel (ECP), which is used as the primary management tool for Exchange Online. The ECP is effective in many respects. For example, its interface is built from "slabs," each of which reveals the necessary UI for specific functionality, such as executing multimailbox discovery searches. The ECP exposes slabs based on users' Role Based Access Control (RBAC) membership. For example, a user who is a member of the Discovery Management role group will see the UI to create, execute, and examine mailbox searches. If you're not a member of this role group, the ECP simply rearranges UI elements to disguise the fact that mailbox searches even exist.

Exchange 2013 management is performed through a much-enhanced version of the ECP called the Exchange Administration Center (EAC), which Figure 1 shows. The EAC uses the same UI framework as the ECP but expands its functionality to include all of the management

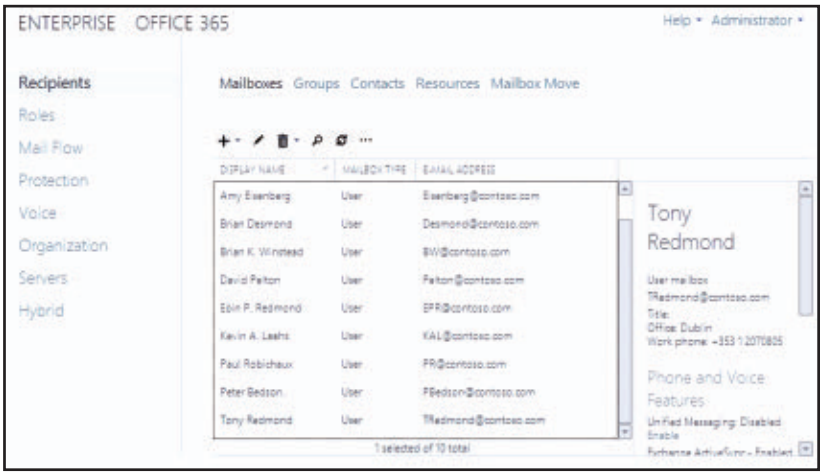


Figure 1
Exchange 2013's Exchange Administration Center

components that the ECP doesn't support, such as DAG management (see Figure 2) and the wizards that automate many aspects of Exchange server management. The EAC follows the design principles for Metro-style interfaces, as does the upgraded version of Outlook Web App (OWA). In addition to being more approachable for inexperienced administrators than the EMC's complex layout is, Microsoft notes that the EAC is far more efficient than the EMC at dealing with a large number of objects and is therefore capable of handling even the largest Exchange deployment.

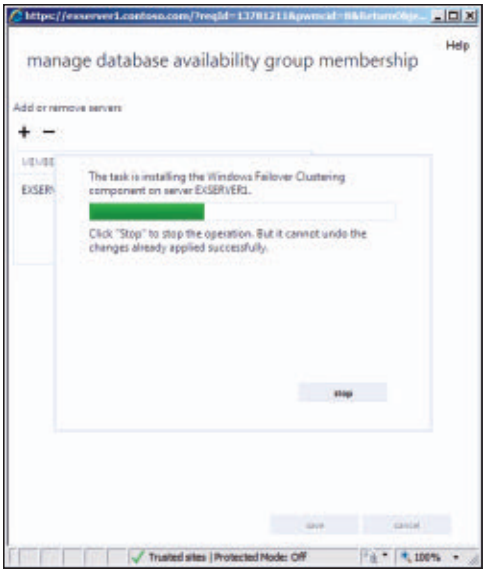


Figure 2
Adding a new server to a DAG

Few will shed many tears at the demise of the EMC. Despite its richness in features, the EMC was slow and unwieldy and had suffered some recent problems when Internet Explorer 9.0 changed an underlying component. It makes more sense for Microsoft to concentrate its efforts on browser-based

management tools that can be used on almost any PC, as well as on other devices such as iPads. In addition, the EAC provides the basis for a common administrative platform shared between on-premises and cloud deployments. The only downside is the loss of the EMC's three PowerShell learning tools. Many administrators used the EMC's ability to display the PowerShell code it executed as a way to become accustomed to PowerShell syntax and constructs.

Modern Public Folders

Microsoft describes the Exchange 2013 implementation of public folders as "modern public folders." Given that the public folder implementation in Exchange 2010 is based on the same design as originally implemented in Exchange Server 4.0 (circa 1996), it's fair to describe the new approach as "modern," especially because the storage model now uses mailbox databases that let public folders take advantage of the development tweaks Microsoft put into refining mailbox databases over the past three releases.

In Exchange 2013, every public folder mailbox holds a copy of the public folder hierarchy. A single public folder mailbox, which is always the first public folder created in the organization, stores a writeable copy of the hierarchy (the master hierarchy). Changes made to the master copy are replicated to the other mailboxes. Access to public folder content is therefore accomplished by first interrogating the hierarchy, followed by a redirect to the specific public folder mailbox holding the content. Unlike in previous versions of Exchange, content isn't replicated to multiple public folder replicas. It always remains in a single distinct location whose integrity is protected by standard Exchange high-availability features.

Moving to this model has many advantages. Public folders have long been the cockroaches of Exchange—unloved but ever-present. As such, they haven't received much attention; some would argue that Microsoft dedicated just enough effort to public folders to keep them alive. Modern public folders are stored in mailbox databases

and are therefore maintained as a core component. Another major advantage is that public folders now enjoy the high-availability features of DAGs. Of course, public folders have enjoyed a multi-copy replication model ever since Exchange 4.0. However, although public folder replication works, it doesn't offer the same kind of advanced replication and problem-solving features that are available in a DAG, such as block mode replication or single page patching.

Exchange 2013 public folder deployment and management will require different techniques. It's too soon to offer a definitive assessment of possible fault lines, but because of the various methods available for deploying public folders, some hiccups are sure to happen along the way—possibly related to electronic forms or to other applications that use public folders for storage.

The migration path to modern public folders goes something like this:

1. Move all user mailboxes to Exchange 2013 servers. Users will still continue to access public folders on an Exchange 2010 server. Users whose mailboxes are on Exchange 2010 or Exchange 2007 servers can't access Exchange 2013 public folders.
2. Run the public folder migration script (PublicFolderToMailboxMapGenerator.ps1) to analyze the existing public folder hierarchy and folder content. You can use this script's output to create an initial set of Exchange 2013 public folder mailboxes.
3. Initiate the process to move public folders to Exchange 2013. The Mailbox Replication Service (MRS) creates public folder mailboxes in the target database and performs the initial population.
4. Background synchronization by the MRS continues to keep two sets of public folders synchronized for up to 30 days. Administrators use this time period to prepare for the final switchover.
5. Administrators trigger the final replication phase. This is similar to the existing functionality in Exchange 2010 where an administrator can resume a suspended mailbox move. The MRS then

performs a final incremental synchronization to ensure that all of the content in the public folders is completely up-to-date, then switches the AD configuration so that users begin to access the Exchange 2013 public folders. All versions of Outlook supported by Exchange 2013 can access public folders in their new location.

6. After the switchover is complete, an organization can't revert to Exchange 2010 public folders.

Although the new public folders are contained in mailbox databases, their content isn't exposed to discovery searches, nor is it possible to apply mailbox retention policies. Microsoft will offer modern public folders as a new feature for Office 365 subscribers. However, because OWA won't support access to public folders until Exchange 2013 SP1, you'll have to use Outlook 2013 to access the new repository.

Data Leak Protection

Microsoft did an enormous amount of work on a broad set of compliance features in Exchange 2010, with archive mailboxes, multi-mailbox discovery searches, an upgraded dumpster, and retention policies. Exchange 2013 adds Data Leak Protection (DLP) to its compliance capabilities.

A simple way to describe DLP is that it stops users from doing stupid things such as including data that they shouldn't share in email messages. For example, it's usually a bad idea to send a credit card number in an email message because this data can be misused if the message is intercepted or ends up with an unintended recipient. DLP tries to identify confidential data in email messages and prevent such data from leaving the organization.

DLP works through policies defined on an organizational level. These policies identify the hallmarks of confidential data that should be protected. DLP is very similar to transport rules in that Exchange examines messages as they pass through the transport pipeline to identify policy violations and then takes whatever action is defined

by the policy. For example, messages can be suppressed, sent to an authorized intermediary such as a manager, protected against unauthorized access with Rights Management Services (RMS), or returned to the sender with an explanation of why a policy has been violated. Code is built in to Outlook 2013 to make it DLP-aware so that potential policy violations can be flagged as messages are composed.

Exchange 2013 includes a set of DLP policies, such as policies that protect Gramm-Leach-Bliley Act data (for financial services), Payment Card Industry–Data Security Standard (PCI-DSS) data (credit card information), and US personally identifiable information (PII) (data that could identify an individual, such as a Social Security number). Custom policies can be created from scratch or imported from a file. Microsoft believes that ISVs will develop market-specific DLP policies that can be sold to companies.

DLP will be very important for some customers, especially those who work in highly regulated industries. Other companies won't regard DLP as important. Adoption will likely be slow because only Outlook 2013 fully supports DLP, much like Outlook 2010 was the only client that could display MailTips when Exchange 2010 debuted.

Site Mailboxes

In some respects, site mailboxes complicate Exchange's collaboration story, if only because even more choices exist for how the sharing needs of groups of users can be met. Site mailboxes are based on SharePoint 2013 and require Outlook 2013 Professional Plus (or OWA). In this implementation, documents reside in SharePoint, and Exchange looks after calendaring and email. A tight link is maintained between Exchange and SharePoint to ensure that new content is synchronized correctly between the two repositories. No hybrid configurations are supported for site mailboxes, which means that the Exchange and SharePoint servers must be deployed on premises.

Setting up site mailboxes is easy. After they're created, new site mailboxes appear in Outlook 2013 as soon as Autodiscover refreshes

the set of resources available to a user. Site mailboxes appear much like shared mailboxes or PSTs, with the obvious difference that any access to a document is processed by SharePoint. The transfer between SharePoint and Exchange is seamless and users can perform all the operations you'd expect, such as dragging and dropping messages from a mailbox to SharePoint or vice versa.

Creating software that meets all possible requirements is difficult in a first release, and site mailboxes are no exception. Several issues exist that could make site mailboxes less successful when deployed.

- Like archive mailboxes, documents associated with a site mailbox that are stored in SharePoint are available only when you're working online. This restriction might not be a huge problem in today's always-connected world; however, there will be times when it's impossible to be online and you might need a document. You can copy documents from SharePoint into a mailbox folder for later use offline—but how likely will you be to remember to do so before a road trip?
- SharePoint supports document versioning, which is a useful feature for teams that collaborate on complex documents. Outlook doesn't support versioning and can display only the latest version of a document. This isn't necessarily a problem unless you need access to an earlier version, in which case you must access documents in the SharePoint site directly rather than going through Outlook.
- Site mailboxes don't respect Exchange retention policies; in addition, site mailboxes can't have archive mailboxes in the same way that a shared mailbox can. Microsoft designed the retention policy and tag model to deal with personal mailboxes. The Managed Folder Assistant (MFA), which is the Exchange component that processes mailboxes to apply retention policies, has no knowledge of the SharePoint sites that underpin site mailboxes. It would be nice if Microsoft extended the retention model to accommodate

site mailboxes in the future so that all of the information available to users could be managed in a single way.

I'm sure that many other operational aspects will be explored as companies deploy site mailboxes. This will certainly be an interesting space to watch.

Client Upgrade: A Necessary Evil

Like previous versions of Exchange, you need to upgrade client desktops to the latest version of Outlook to be able to exploit all the features that Exchange 2013 supports. Features such as DLP and site mailboxes simply won't surface in earlier versions. Although Outlook 2013 has some useful new features that make sense (such as the ability to reply to a message within the reading pane) and enhance the user interface (such as the ability to display expanded contact information using data retrieved from multiple social networking sources or the ability to display weather information for meetings), the upgrade to Outlook 2013 will be a hard sell within many companies—particularly because the new Metro-style UI will provoke worries about user training and support similar to those when Office 2007 introduced the Ribbon interface.

Older clients can connect to Exchange 2013, but this release marks the end of the road for Outlook 2003. Microsoft did a lot of work to retrofit support for Outlook 2003 into Exchange 2010 but hasn't brought that work forward into Exchange 2013. Equipped with the latest patches, Outlook 2010 and Outlook 2007 work just fine as long as you don't want to use the new Exchange 2013 features. It remains to be seen whether Microsoft will issue a service pack or other update to reveal features such as DLP in Outlook 2010 and Outlook 2007 in the same way that the company eventually supported Exchange 2010 archive mailboxes for Outlook 2007.

OWA continues to get better and better. Although some might be enthused by the addition of inline editing for new messages, which

Figure 3 shows, the OWA headline feature for Exchange 2013 is the addition of offline access, which OWA switches into if a network connection is unavailable. To some degree, adding offline access is a nod to Gmail, which introduced offline access mode in 2011. Offline

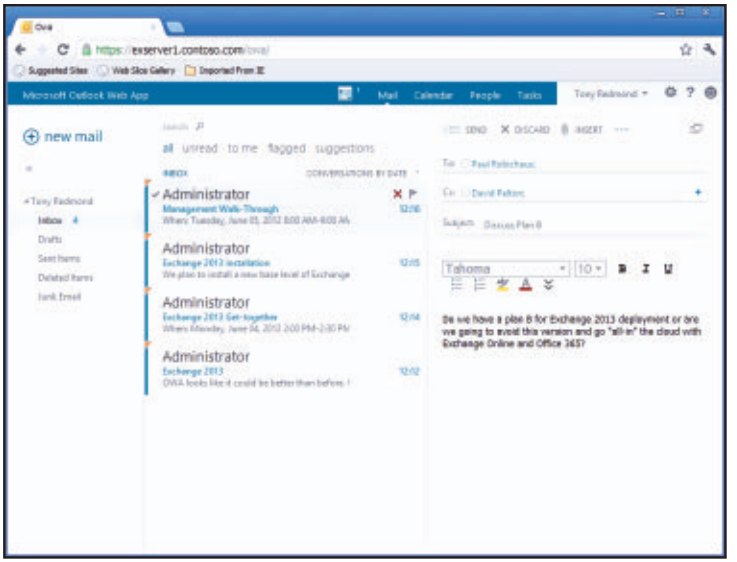


Figure 3
Exchange 2013 Outlook Web App

storage is standards-based and is managed by the browser you use. If your browser supports HTML5 IDB, OWA will use it for storage; if not, OWA will use WebSQL. You need to be running IE 10.0, Chrome 16.0 or later, or Safari 5.1 or later to use offline access because these are the only browsers that currently support the storage mechanism.

Even more interesting is the way OWA morphs itself to support three distinct screen form factors (phone, slate, and traditional PC). The UI is Metro-based and touch/gesture-capable across the width of the screen; it has an advanced HTML5-based mode that facilitates video display. The two traditional modes (premium and reach) continue to let OWA support the widest possible range of browsers. Although the OWA support matrix is a tad more complex because of the multiple form factors, IE, Chrome, Firefox, and Safari all support the premium interface.

Exchange Online

Exchange Online is a major part of the Office 365 value proposition, so it's no surprise to learn that Exchange Online will include the new features enabled by Exchange 2013 soon after general availability. Microsoft hasn't set a firm date for the update yet but will advise tenant administrators when to expect upgrades to commence. The company will allow tenant administrators to select the most appropriate upgrade time within a window spanning a couple of months. Tenants can even opt to run a pilot deployment for a select group of users before full deployment begins. This feature is based on scheduling batches of mailbox moves. Exchange 2013 marks the first time that Office 365 has been through a major application functionality upgrade—so it's good that Microsoft has considered how to minimize disruption for customers during the transition.

The Big Upgrade Question

Exchange 2013 includes numerous improvements that I haven't discussed here. For example, the Exchange content-indexing subsystem is replaced by a FAST-based search engine that extends over Exchange 2013, SharePoint 2013, and Lync 2013 to provide a single enterprise-class search capability across multiple data sources. This upgrade would certainly merit much discussion in another release—but such are the changes in Exchange 2013 that this improvement is merely mentioned in passing.

As always, when Microsoft releases a brand-new version of a popular server application, we must ask whether there's a compelling reason to upgrade. In this case, the answer for companies running Exchange 2010 is probably No—unless they have a pressing need to use one of Exchange 2013's new features and the necessary financial and technical resources to deploy new hardware and new software (Exchange and SharePoint), upgrade clients, train and support users, and so on. But if you're running Exchange 2003, it's definitely time to move to new technology, and it makes sense to consider an

early upgrade to Exchange 2013. The same argument can be made for Exchange 2007 deployments. Although these servers did a good job in their time, that time is quickly running out.

Of course, companies faced with the complexity and cost of migrating to Exchange 2013 might simply conclude that now is a good time to move some or all of their user population to Office 365. Moving to Office 365 isn't free of charge; costs will be incurred to plan, prepare, and execute all the steps necessary to set up a new tenant domain, establish interoperability with on-premises Exchange, establish single sign-on (SSO) using Active Directory Federation Services (AD FS), move mailboxes to the cloud, and figure out details such as the effect on other applications. But the whole point of going through this pain is that after you migrate to Office 365, Microsoft will take care of the heavy lifting of server and software maintenance from that point on and you'll be able to take advantage of new features and functionality soon after release without having to go through a traditional migration. The steadily improving reliability record of Office 365, combined with the release of Office 2013 apps, will create a real decision point for companies as they chart their long-term future for email services.

If you can cope with the migration and can make use of the new features, Exchange 2013 will be worth the effort.

Old Habits Die Hard

If you can cope with the migration and can make use of the new features, Exchange 2013 will be worth the effort. The implementation seems solid, and Microsoft has tested the heck out of this release to prepare for its introduction in the Office 365 cloud service. Still, I think most Exchange admins will opt to wait for SP1. After all, in the past three major versions, Microsoft has substantially improved the initial Exchange release with the first service pack. Why spoil what has become such a long-standing habit? ■

InstantDoc ID 143174

New Ways to Enable High Availability for File Shares

Windows Server 2012 changes how file sharing works

John Savill

is a Windows technical specialist, an 11-time MVP, and an MCITP: Enterprise Administrator for Windows Server 2008. He's a senior contributing editor for *Windows IT Pro* and his latest book is *Microsoft Virtualization Secrets* (Wiley).

Email

Twitter

Website

What's the coolest feature in Windows Server? My guess is that file-sharing services didn't make your top five. But that might change with Windows Server 2012. File and Storage Services combined with the new Server Message Block (SMB 3.0, formerly SMB 2.2) protocol introduce some truly great new features that completely change how file sharing works and that can be used in a highly available configuration. In this article, I'll focus on two new capabilities of file services in a failover cluster: SMB Transparent Failover and SMB Scale-Out. I'll show how you can use these capabilities together to provide a file services environment that can be used for the most demanding workloads, including hosting Microsoft SQL Server databases and Hyper-V virtual machines (VMs).

File Services in a Failover Cluster Environment

Before I focus on the new features, I want to quickly describe how file services work in a failover cluster environment, which allows highly available file servers and, more specifically, file shares. A Server 2012 failover cluster consists of as many as 64 servers (up from 16 in Windows Server 2008 R2) that have the Failover Clustering feature installed and are configured to share a common set of storage and services.

The services that are defined in a cluster can be moved between the servers (aka nodes) in the cluster. These services consist of various resources, such as IP address, network name, storage, and the actual service, such as a file server, print server, VM, Microsoft Exchange Server

mailbox server, and so on. Services can be moved between nodes in the cluster in a planned situation or in an unplanned scenario, such as a server failure. In the latter case, services that ran on the failed server are automatically redistributed among the remaining nodes in the cluster.

Figure 1 shows a four-node cluster and a file server resource. The file server offers a single file share, which stores its content on an NTFS-formatted LUN. The LUN is a block of space from the shared storage, to which all the nodes in the cluster can connect. The file server, and thus the file share, is online initially from the third node of the cluster. This node also mounts the LUN, which contains the file server content. During any failure, the file server moves to the fourth node, which also mounts the LUN, which is required to offer the share content. The LUN must be mounted by whichever node is offering the file server that corresponds to the content because NTFS is a shared-nothing file system and can't be accessed concurrently by more than one node. Therefore, when a file server moves to another node, the LUN must be moved between nodes as well.

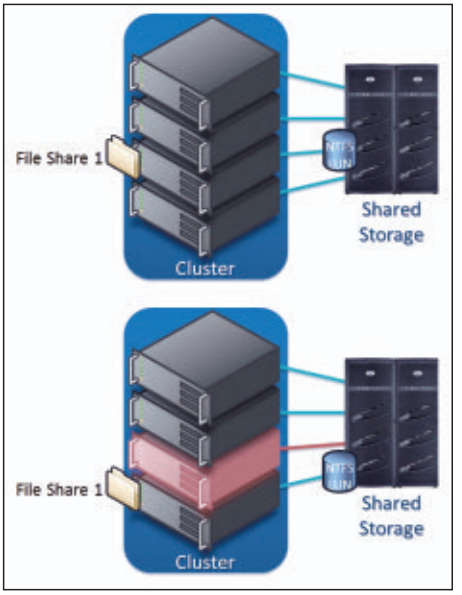


Figure 1
Basic failover cluster with a service moving between the nodes

SMB Transparent Failover

The previous example involves challenges to using a file share that is moved between nodes in the cluster in planned and unplanned scenarios. First, when a file on a file share is used by an application, handles are typically created to allow an application to access the file and potentially to lock the file to stop another application trying to write at the same time. In addition, the handle defines how data is accessed

and specifically whether data can be buffered on the file server, which might help to enhance performance. With Server 2008 R2 and earlier, any handles and locks are lost when the file server moves to another node. In general, this behavior doesn't cause a huge problem for regular users accessing Microsoft Word documents. But that wouldn't be true if this was a database used by SQL Server.

The second challenge involves the time that is needed for a file server client to recognize that a file server is no longer available and to start taking recovery steps. TCP/IP timeout values can typically cause an interruption of about 40 seconds—unacceptable when server applications store data on file shares. For those 40 seconds, all activity that requires file I/O to the share pauses—an event commonly known as a brownout. Removing these challenges is vital for SMB. If server applications such as SQL Server and Hyper-V are going to use SMB file shares, they can't lose data handles or suffer 40-second pauses in I/O!

The new SMB Transparent Failover feature addresses both issues. The feature enables continuously available file shares for SMB 3.0 clients, removing the loss of handles during a failover and reducing the time needed to detect that a file server has moved to another node, thus reducing brownouts.

Keeping file shares available. SMB Transparent Failover consists of several configuration changes and new technologies. One benefit that file servers traditionally offer clients is buffering of data writes to disk. This element provides faster acknowledgments to client write requests because the file server caches the write operation in its volatile memory (meaning that if the server loses power, it loses the data), tells the clients that the data is written so that the client can carry on its work, then performs the write in the most optimal way. Certain applications always open handles with this caching disabled, through the use of the FILE_FLAG_WRITE_THROUGH attribute, ensuring that data is always written to the actual disk before receiving acknowledgment and avoiding any volatile cache. SMB Transparent Failover

sets the FILE_FLAG_WRITE_THROUGH as the default for all created handles, eliminating the use of volatile memory cache. Now, there might be some performance implications because the cache is no longer used, but the assurance of data integrity is a good trade for the possibility of a slight performance degradation.

The second change that SMB Transparent Failover makes is how the OS manages file handles. File handles typically are stored in the memory of the file server. However, if a node fails and the file server moves to another node in the cluster, the handles are lost—bad news for the using application. In addition to storing the handle state in memory, SMB Transparent Failover backs up the handle state in the Resume Key Database, in the System Volume Information folder of the disk on which the file resides and that the handle is referencing. Storing the handle information on disk maintains the handle state when the file server moves between nodes in the cluster. However, because disk access is multitudes times slower than memory, heavy metadata–generating workloads such as creating, deleting, renaming, extending, opening, and closing files cause additional I/O in the Resume Key Database, removing available I/O from normal disk usage. But again, this tradeoff is acceptable to ensure that handles are maintained when moving file servers between nodes. (See the sidebar "What About Performance?" for my rationale on this exchange.)

What About Performance?

I've talked about how the changes that SMB Transparent Failover makes could introduce a slight performance penalty because of the bypassing of write cache and the increasing of I/O from metadata-heavy operations. This penalty might sound fairly off-putting. But in reality, many key server applications that would benefit from this technology, such as Microsoft SQL Server and Hyper-V, specify the use of FILE_FLAG_WRITE_THROUGH to bypass write cache anyway. Also, such applications perform very few metadata operations. Rather, they read and write to the data of the file, so they won't be much affected by the disk-based Resume Key Database. These changes are more likely to have an effect on user workloads, such as opening Microsoft Office documents. Such workloads aren't the focus of this feature. ■

Reducing brownouts. To meet the second challenge and reduce the time that an SMB client takes to realize that its TCP connection has died, the cluster must be proactive. The cluster must notify SMB clients that connect to a cluster-hosted share whenever the hosting file server moves to another node. That way, the client can more quickly reconnect. Enter the new SMB Witness capability, which operates something like this:

SMB Client: "I want to connect to this share on your ServerA."
SMB ServerA: "OK, you are connected. This share is hosted on a cluster; let your SMB Witness process know."
SMB Client Witness: "Great! Tell me about all the nodes in the cluster."
SMB ServerA: "Here is a list of all the nodes in the cluster: ServerA, ServerB, ServerC . . ."
SMB Client Witness: "Hey, ServerB. I am connecting to this share with this IP address on ServerA. I want to register with you so that you can tell me if something happens to ServerA or if the file server moves."
SMB ServerB: "Sure, I'll let you know."

After this exchange, if anything happens to that file server in the cluster, the SMB client is notified proactively via its SMB Witness process and can reconnect far more quickly than TCP/IP timeouts would allow. The new time to detect and react to a failure or file server move is likely in the range of 5 to 7 seconds instead of 40 seconds.

When you use the Failover Cluster Manager, Server Manager, or Windows PowerShell to create a file share on a Server 2012 cluster file server, SMB Transparent Failover is enabled by default on that share. (Note that this isn't the case when you create the share by using Explorer or the Net Share command, neither of which understand SMB Transparent Failover.) Windows 8 or Server 2012 clients, which are SMB 3.0-compatible, will then use the SMB Witness capability and will open sessions to use write-through handles.

You can use PowerShell to confirm that this process is happening. In my lab, I have two nodes in a cluster with a file server resource and a share. I connected from my client machine, and from an elevated PowerShell window I executed the following command on a node in the cluster:

```
PS C:\> get-smbwitnessclient | select clientname,
  fileservernodename, witnessnodename
clientname   fileservernodename  witnessnodename
----------   -----------------  ---------------
savdalwks08  WIN8FC01           WIN8FC02
```

As you can see, the output shows the name of my client computer (savdalwks08), the file server the client is connected to (Win8FC01), and the node with which it has registered for notification (the witness, Win8FC02). (Another option is to use the Get-SmbOpenFile PowerShell cmdlet and look at the ContinuouslyAvailable property.)

To view a list of all the administrator-created shares and to determine whether they are configured for continuous availability, use the following PowerShell code:

```
PS C:\> Get-SmbShare | Where {$_.Scoped -eq "true" -and
  $_.Special -ne "True"} | Sort ClusterType | Format-Table
  Name, ScopeName, ClusterType, ContinuouslyAvailable, Path
Name       ScopeName   ClusterType  ContinuouslyAvailable Path
----       ---------   -----------  --------------------- -----
NonCSVData WIN8FSTRAD  Traditional  True E:\Shares\NonCSVData
DataCSV    WIN8FSSCOUT ScaleOut     True C:\ClusterStorage\Vo...
```

SMB Scale-Out

Using file servers in a cluster hasn't changed fundamentally since its introduction. Only one node in a cluster can mount and host shares for a particular NTFS-formatted LUN at any one time. This single-node offering of services can limit scalability and introduce delays

because LUNs must be dismounted, moved, and mounted when the file server resource moves. This necessity has led storage and file services architects to make some sub-optimal design decisions when planning their clusters, to avoid nodes sitting idle.

Consider an organization that wants to share one NTFS volume but requires the share to be highly available. This scenario requires at least two hosts in a cluster, but only one host can actually offer the share. To avoid an active/passive situation in which one host does nothing, storage admins divide the LUN into two, create two NTFS volumes, then create two file servers in the cluster, each with its own share. This setup allows each node to offer one share and to host the other node's share during a failure. This way, both hosts are working—but the storage is now divided in ways the organization might not want. In addition, if you don't divide the content correctly, one share might get more traffic than the other, causing an imbalance and potentially forcing you to move data around. And this is with just two nodes. Now imagine that you have four nodes, as Figure 2 shows, or eight nodes; that's a lot of separate LUNs, NTFS volumes, and shares just to keep all the nodes in the cluster busy.

The root of the problem is that NTFS volumes don't share and can't be used by more than one node simultaneously. This issue was partially solved in Server 2008 R2, which introduced Cluster Shared Volumes (CSVs). I wrote about CSVs in "Introduction to Cluster Shared Volumes," so I'm not going to discuss it in detail here. Basically, CSV enables a single NTFS-formatted LUN to be written to and read from all nodes in the cluster simultaneously, through some clever behind-the-scenes mechanics. CSVs in Server 2008 R2 were supported

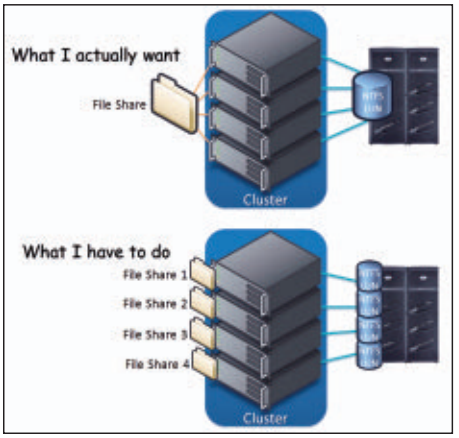


Figure 2
Required compromise with traditional clustered file servers

only for the storage of Hyper-V VMs running on the Hyper-V hosts in the cluster that contained the CSVs.

Server 2012 expands the use of CSVs to a new type of cluster file server, namely the new SMB Scale-Out file server. The file server type—Scale-Out or Traditional (i.e., the existing file server model)—is selected at the time of creation. When you create a new file server of the Scale-Out type, you must create the shares on folders that are stored on CSV volumes. In Server 2012, NTFS volumes that have been CSV-enabled show as file system type CSVFS instead of NTFS. In reality, the file system is still NTFS, but the change in file-system labeling makes it easy to distinguish between volumes on disks that are CSV-enabled (i.e., CSVFS) and those that are not (i.e., NTFS). Remember that a CSV is available to all nodes in the cluster simultaneously, so this created share can now be offered by all the nodes in the cluster at the same time, and all the nodes can get to the content. When creating a Scale-Out file server, you don't need to specify an IP address. The IP addresses for the interfaces that are configured for client access on the cluster nodes are used; all nodes offer the service.

Another great feature is the ability to use SMB Transparent Failover to move a client from one node that offers a Scale-Out file server to another node, without any access interruption. Suppose, for example, that you want to place a node in maintenance mode. The following command moves a specific SMB client from one node to another; you can easily use PowerShell to execute this command for all clients that use a specific node in the cluster.

First, I determine which server an SMB client is using (we used this command previously):

```
PS C:\> get-smbwitnessclient | select clientname,
  fileservernodename, witnessnodename
clientname     fileservernodename     witnessnodename
----------     ------------------     ---------------
savdalwks08    WIN8FC01               WIN8FC02
```

Now, I move that client to my other server:

```
PS C:\> Move-SmbWitnessClient -ClientName savdalwksØ8
  -DestinationNode Win8FCØ2
```

To verify that the move happened, I rerun my command. I see that the client has moved to the other node in my cluster, and the witness is now my original server. (Because the file server and witness can't be the same server, that wouldn't be useful!)

```
PS C:\> get-smbwitnessclient | select clientname,
  fileservernodename, witnessnodename
clientname     fileservernodename     witnessnodename
----------     ------------------     ---------------
savdalwksØ8    WIN8FCØ2               WIN8FCØ1
```

What does this output mean? Refer again to Figure 2. You can now create that single big LUN that you wanted, with one NTFS volume that all four nodes share simultaneously. (Microsoft supports as many as eight nodes offering one SMB Scale-Out file server.) This capability simplifies management, eliminating the need to associate numerous separate LUNs, shares, and IP addresses with each file server. So why does the traditional file server type still exist?

As I mentioned previously, CSV performs some clever mechanics to enable one NTFS volume to be written to and read from all nodes in the cluster simultaneously. One of the cleverest parts is handling metadata writes to NTFS volumes, which is the biggest problem with multiple computers concurrently using one NTFS volume. Having two servers writing metadata at the same time is likely to cause a corruption. CSV solves this problem by having a coordinator node for each CSV disk. This node mounts the disk locally and performs all metadata activity on behalf of the other cluster nodes that send metadata writes over the cluster network to the coordinator. (These other

nodes can still directly access the disk for standard data I/O.) This metadata redirection over the network can cause latency in operations. That's why the SMB Scale-Out file server is targeted at key application server workloads such as SQL Server and Hyper-V, which are very light on metadata activity and focus on data I/O. When you contrast the server application I/O characteristics with those of a typical information worker using Microsoft Office documents, the I/O for an information worker is typically 60 to 70 percent metadata operations. That's a lot of data being redirected. I'm not saying that using an SMB Scale-Out file server in such a scenario won't work or will perform badly if architected correctly, but it's certainly something to consider. At this time, the Scale-Out file server is recommended only for server applications like SQL Server and Hyper-V.

There's another reason that the Scale-Out file server is unsuitable for storing Office documents and other user data. The Windows file server platform is often used because of features such as quotas, file screening, file classification, BranchCache, and (in Server 2012) data deduplication. None of these features are available on a Scale-Out file server. Server applications don't care about such features.

Closing Thoughts

When you combine the Scale-Out file server with the SMB Transparent Failover feature, you get a file services platform that allows multiple servers to serve the same share with the same content. The result is great scalability for clients and a resiliency that was previously impossible. Although Scale-Out focuses mainly on SQL Server and Hyper-V workloads, expect more types of workloads to be tested and recommended over time, offering customers many new options in their storage and overall IT architectures. ■

InstantDoc ID 143299

Microsoft Releases Windows Server 2012

Improvements in storage, virtualization, and management are worth a look

Windows Server 2012, arguably the most significant server release Microsoft has ever offered, will be generally available for evaluation and purchase to customers around the world on September 4, 2012. Windows Server 2012 offers a simplified licensing model that includes all features of the OS in all editions of Server. You'll see improved management capabilities in Server Manager and PowerShell. Storage improvements are numerous, and Hyper-V enhancements include scalability, live migration upgrades, and storage live migration capabilities. *Windows IT Pro* brings you ongoing coverage of Server 2012, with in-depth treatment of significant features, breaking news, and analysis. Visit our Windows Server 2012 page for the latest news and technical features. ■

InstantDoc ID 143935

Top 10 Windows Server 2012 FAQs

1. How do I enable and view the Windows Server 2012 Hyper-V metric information?
2. What is the difference between installing Windows Server 2012 as Server Core or server with a GUI?
3. How many processors are supported on supported Linux virtual machines with Windows Server 2012?
4. Will Windows Server 2012 let you shrink and expand virtual hard disks (VHDs) while online?
5. What are the new Hyper-V limits with Windows Server 2012 Release Candidate?
6. Is the Windows Server 2012 data deduplication feature also available in Windows 8 client?
7. I have virtual machines running on Windows Server "8" Beta and want to move to the Windows Server 2012 Release Candidate—what do I need to do?
8. I notice Windows Server 2012 virtual machines have a Smart Paging File Location—what is the Smart Paging File?
9. I have Windows Server "8" Beta volumes dedepulicated. Can I just install the Release Candidate and still access my data?
10. Can I copy my customized Windows 8 and Windows Server 2012 Server Manager configuration to other users and computers?

Windows Server 2012 Articles

- Microsoft Releases Windows Server 2012 to Manufacturing
- Top 10 Windows Server 2012 Storage Enhancements
- Is Microsoft Trying to Kill Windows Server?
- Getting Around in Windows Server 2012, Part 1
- Shared-Nothing VM Live Migration with Windows Server 2012 Hyper-V
- Windows Server 2012 Simplifies Active Directory Upgrades and Deployments
- Windows Server 2012 Storage Spaces
- Video: Windows Server 2012 Storage Spaces Demo
- How Windows Server 2012 Improves Active Directory Disaster Recovery
- Introducing a Simpler Windows Server
- Windows Server 2012 Will Have Feature Parity Across All Editions
- Windows Server 2012 Is Good News for IT
- Top 10 New Features in Windows Server 2012
- Understanding Windows Server 2012 Hyper-V Networking Changes
- Windows Server 2012 Active Directory Moves Forward
- Microsoft's Jeffrey Snover Discusses Windows Server 2012
- Windows Server 2012 Beta Introduces ReFS: Resilient File System
- Exploring Windows Server 2012: Dynamic Access Control
- What's New in Windows Server 2012 Active Directory
- Server Manager in Microsoft Windows Server 2012
- Windows Server 2012: A Leap Ahead

www.windowsitpro.com/windows-server-2012

Hiding Active Directory Objects and Attributes

Use normal permissions to grant or remove access to AD data

Guido Grillenmeier

is a chief engineer within the Enterprise Services Group at HP. He is a Microsoft Directory Services MVP, a Microsoft Certified Architect, and the coauthor of *Microsoft Windows Security Fundamentals* (Digital Press).

Email

Active Directory (AD) allows delegated administration of users, groups, or computers, according to any security principal. But default AD permissions can complicate the task of making specific data visible to only those users who need to see it. AD data-hiding options can be based on typical AD permissions, a special AD permission feature called List Mode, or a little-known option called the confidentiality bit.

Part 1 of this multi-part series, "Hiding Data in Active Directory," explains the challenge of hiding data in AD and goes into details such as AD's default security settings and property set definitions. In this article, I'll describe how to use normal permissions to hide objects and attributes. Future articles will cover enabling List Mode in the AD forest and adjusting the default security of objects in AD.

Using Normal Permissions

You can use the normal capabilities of AD permissions to ensure that users can view and access only their entitled objects and attributes. The principle is straightforward: If a user isn't authorized to view an object or attribute, AD won't display the information to the user.

To view the objects in an organizational unit (OU), a user must have at least the List Contents permission on the OU. As I described in detail in the first part of this series, various security principals, including Authenticated Users, are granted the read permission on any newly created OU. These principals are also granted the List

Contents permission on an OU, although AD doesn't enforce this permission by default. The default read permission is a combination of permissions, including List Contents, as Figure 1 shows.

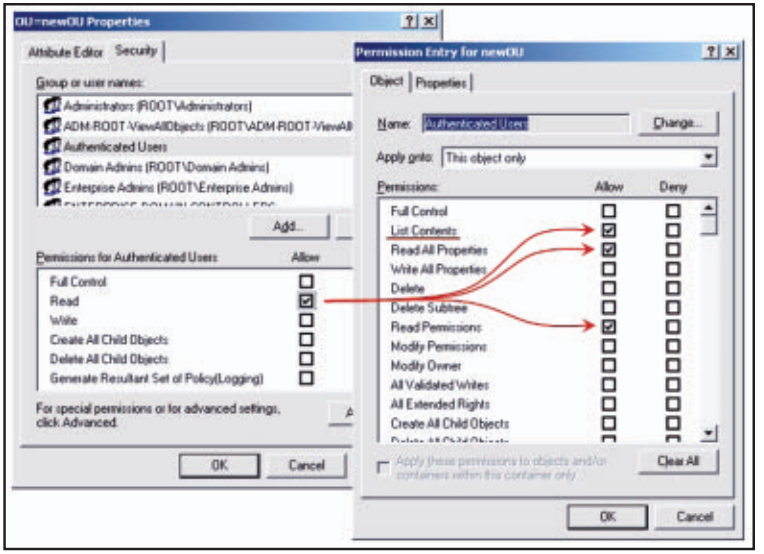


Figure 1
Set of permissions granted the read permission

By default, the List Contents permission grants sufficient rights to list all objects in an OU. This doesn't mean that a user can automatically view the attributes of all objects in an OU; to do this, the user requires read permissions on the respective attributes of the objects within the OU. But the administrator has no control over which *objects* are displayed. You can change this behavior by enabling the List Mode access in AD, which I describe in the next section.

If the List Contents permission for Authenticated Users is removed from an OU, then a query for all user objects in the AD forest won't return the objects in that OU. The same is true when using the Windows object picker to list objects. The object picker is typically used to add users to groups or to select a security principal when granting permissions to resources. By default, the object picker displays all objects in the containers to which the current user has List Contents permission (and which are appropriate for the task the user is performing).

Removing the List Contents permission for Authenticated Users from an OU hides all the objects in that OU for all users in AD, unless the users are members of other groups that are specifically granted the appropriate permissions. Explicitly denying the List Contents permission to a group has the same effect. But to keep things simple and comprehensible for any systems administrator, it's better to work with positive permissions (allow) instead of negative permissions (deny).

You can easily remove the permission for a single OU through the Microsoft Management Console (MMC) *Active Directory Users and Computers* snap-in or the ADSI Edit GUI, by using the Security tab of an object's property. To do so from the command line, you can use the Dsacls utility that comes with the OS. (Dsacls is part of the Windows Server support tools. See "Dsacls Syntax" for more information.)

This command can't remove single permissions directly. To do so, you must first remove all permissions for the respective security principal and then assign new ones. (Note that although most companies are still happily using Dsacls, Windows Server 2008 R2 and later provide new AD cmdlets for Windows PowerShell, as I discuss in the sidebar "Managing Active Directory Permissions via Windows PowerShell." These cmdlets offer new options for managing the security of AD objects.)

Removing all permissions for a security principal from the command line shouldn't be taken lightly, especially if you don't know exactly which permissions the security principal has on the object. You should first generate a report of the ACLs of an object so that you can more easily reset them if needed. A couple of tools are available to do this; all of them have their advantages and disadvantages. The Microsoft Dsrevoke tool achieves good results by allowing you to report on the ACLs for a specific security principal. However, the tool can't do so for well-known security principals such as Authenticated Users or for built-in ones such as Administrators. Furthermore, this tool is supported only on Windows Server 2003 and earlier. Dsacls always list the permissions for all security principals, as Figure 2 shows, yet that's better than not listing any permissions at all.

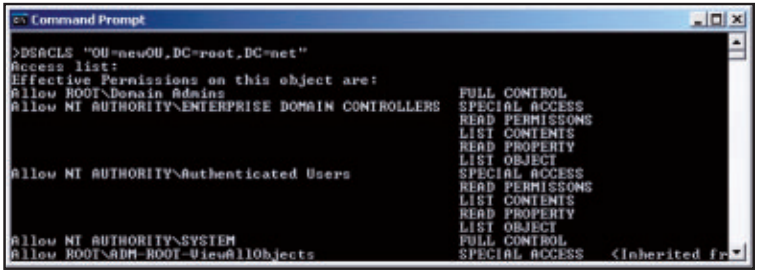


Figure 2
Partial result of Dsacls listing ACLs on an OU

Removing Permissions

To remove the List Contents permissions for Authenticated Users on a new OU, use the following command:

```
dsacls <DN of object> /R <security principal>
```

In our example, this command would look like this:

```
dsacls "OU=newOU,DC=root,DC=net" /R "Authenticated Users"
```

Afterwards, you must reset all the default object permissions (i.e., read permissions, Read All Properties, List Object) except for the one that you removed. To do so, use the following command:

```
dsacls <DN of object> /G <security principal>:RCRPLO
```

In our example, the command would look like this:

```
dsacls "OU=newOU,DC=root,DC=net" /G "Authenticated Users":RCRPLO
```

To combine both commands, you'd typically create a batch file and use variables. If you want to run the commands via a single command-line statement, you can use the && command:

```
set DN="OU=newOU,DC=root,DC=net"&& set SP="Authenticated Users"
  && dsacls %DN% /R %SP%&& DSACLS %DN% /G %SP%:RCRPLO
```

(Any character preceding the && command is part of the previous command. This command is especially tricky when used after setting a variable via *set*, when a trailing space is added to the variable.)

The outcome of these changes is that, if the requesting user doesn't have or is denied read access to an attribute, AD doesn't return any data that's stored within this attribute. The GUI that comes with AD either displays an empty field in the MMC *Active Directory Users and Computers* snap-in or displays <Not Set> for the attribute value when using ADSI Edit, as Figure 3 shows.

The special challenge of controlling read access at the attribute level in AD is a consequence of the grouping of attributes in permission property sets and the vast amount of explicit default permissions that are assigned to new objects in AD.

What if, for example, you want to restrict access to the homePhone attribute to members of the HR department? Looking back at "Hiding Data in Active Directory," you can see that the homePhone attribute is one of the 47 attributes that belong to the Personal Information property set and that Authenticated Users are granted read permissions to this property set for any new user object in AD. Removing the read permission from a single attribute isn't easy if the attribute is a member of a property set that has been granted read permissions on the object. Instead, the read permission for the whole property set needs to be removed and replaced

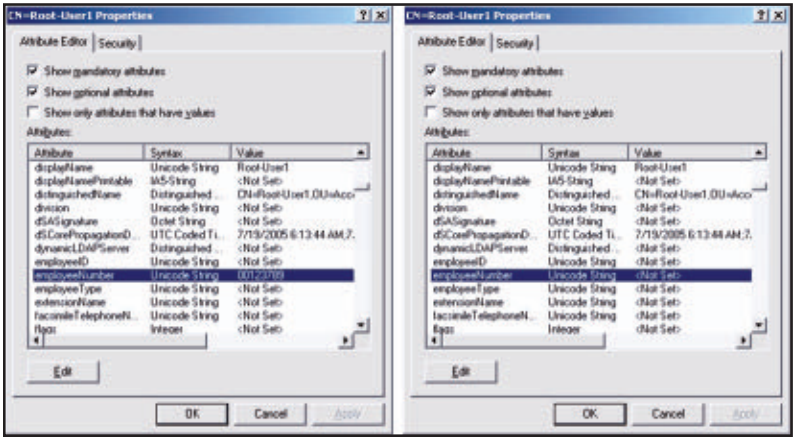


Figure 3
Content of attributes with read access (left) and without read access (right), using ADSI Edit

with a separate read permission for all properties *except* the one that isn't required. To remove the permission for Authenticated Users to read a user's homePhone attribute, you'd need to replace the read permission for the Personal Information property set with 46 separate read permissions for all the other attributes in the property set. Another option is to adjust the attributes that belong to a property set, but for now let's assume that you don't want to adjust the property set.

Even though you want to generally avoid using deny permissions, in this scenario working with a deny read permission on the homePhone attribute of the respective user objects for a security group that contains all users except the HR department is the efficient option. Let's call this group non-HR-users. However, creating such a group and keeping it up-to-date is a challenge on its own. Another challenge is that you can't simply set the required deny permission at the OU level or the domain level and allow the respective user objects to inherit it. As described previously, the explicit allow permissions that are granted to Authenticated Users directly on the user object will override the inherited permission from the parent objects. So you must add an explicit deny read permission for the non-HR-users group to all user objects in the AD forest.

More Dsacls

Presuming that you don't want to set the explicit deny permission to all objects by clicking through the GUI for hours, you can achieve the same task fairly easily by using the Dsacls command-line tool. Because you must set explicit permissions on each user object to achieve your goal, you need to run separate Dsacls commands—each with the distinguished name (DN) of the user object for which you need to set the deny permission. There are various ways to retrieve the list of user object DNs: You can use the Dsquery command-line tool that comes with Windows 2003; you can also use this tool to query a Windows 2000 domain controller (DC), if you still have one. (You can find more information about using Dsquery on the Microsoft website.)

To set the permission to deny read access of the homePhone attribute on a single user object, you can use this command:

```
dsacls <DN of object> /D <security principal>:
  RP;homePhone
```

For our example, the command would look like this:

```
dsacls "CN=Doe\, John,OU=newOU,DC=root,DC=net" /D root\
  non-HR-users:RP;homePhone
```

For multiple objects, you must first create a list of DNs and save them to a file. You can use Dsquery:

```
dsquery user <StartNode> > queryresult.txt
```

For our example, the command would look like this:

```
dsquery user OU=newOU,DC=root,DC=net > queryresult.txt
```

Next, after ensuring that the query results meet your expectations, you must perform a *for* loop to execute the Dsacls command against all objects in the file:

```
for /f "delims=" %I in (queryresult.txt) do DSACLS "%~I" /D root\
  non-HR-users:RP;homePhone
```

This command sets the desired permission for all objects that are listed in the queryresult.txt file.

In summary, keep the following in mind when using the default AD permissions to hide objects and attributes:

- You must understand the default and current permissions that are granted to an object and its parent container. If a user isn't

granted the List Contents permission on a container object, then the objects in the container aren't visible.
- You must understand how attributes are granted permissions by property sets. An attribute isn't visible if a user doesn't have or is denied read access to it.
- If permission for an attribute must be denied and that attribute is also part of a property set that's explicitly granted the permission, then the deny permission for the attribute must be explicitly set for all objects on which it's supposed to take effect.

Know the Possibilities

Using the normal AD permissions to hide data in AD is certainly possible. Two more fairly straightforward options for hiding data are available: List Object mode and changing the default security descriptor of objects in AD. I'll describe these methods in a subsequent article. ■

InstantDoc ID 143605

Managing Active Directory Permissions via Windows PowerShell

In Windows Server 2008 R2, Microsoft introduced Windows PowerShell cmdlets to manage most aspects of AD, including managing AD object and attribute permissions. You need to use the Get-ACL and Set-ACL cmdlets, which treat AD objects the same way as file system or registry objects. There are clear benefits to using the same cmdlet for any type of system object. However, these benefits come at the cost of complexity. It's still easier to manage AD permissions by using Dsacls, although Microsoft will further invest into improving any aspect of Windows management via PowerShell, so it won't hurt to get up to speed with the PowerShell cmdlets to manage AD, including AD permissions.

If the following code means nothing to you

```
$ace = new-object System.DirectoryServices.ActiveDirectory
  AccessRule $sid,"CreateChild","Allow",$objectguid
```

then check out the complete sample of adding object-specific permissions in AD via PowerShell on the Microsoft Active Directory PowerShell blog. Alternatively, you can check out the free Quest PowerShell cmdlets for AD, which offer a variety of powerful, AD-specific permission-mgmt functions, such as Get-QADPermission, Add-QADPermission, and Remove-QADPermission. See PowerGUI.org for more information. ■

InstantDoc ID 143896

Generating Random Passwords in PowerShell

This simple script helps you pump up password strength

Bill Stewart

is a scripting guru who works at Emcore in Albuquerque, New Mexico. He's a contributing editor for *Windows IT Pro* and a moderator for Microsoft's Scripting Guys forum. He offers free tools on his website.

Email

Website

In May of 2009, I wrote an HTML Application (HTA), RandPass.hta, that uses JScript code to conveniently generate random passwords (see "Random Passwords on Demand"). The HTA has four check boxes that you can use to specify which character classes (uppercase, lowercase, numbers, and symbols) the HTA can include in the generated passwords. The operative words are *can include:* It doesn't force the inclusion of the selected character classes in the passwords it generates. The check boxes merely create a list of characters to choose from.

I wanted the ability to generate random strings just by using RandPass.hta, but from the Windows PowerShell command line. I also wanted to improve on the algorithm that RandPass.hta uses: Rather than specifying character classes that *might* appear in the password strings, I wanted to specify classes that *will* appear in the password strings. To accomplish this goal, I wrote Get-RandomString.ps1.

Making a Good Thing Better

The command-line syntax for RandomString.ps1 is as follows:

```
Get-RandomString.ps1 [[-Length] <UInt32>] [-LowerCase]
  [-UpperCase] [-Numbers] [-Symbols] [[-Count] <UInt32>]
```

The Length parameter specifies the length; for example,

```
-Length 32
```

means that Get-RandomString.ps1 will generate random strings of 32 characters. If you don't specify this parameter, the default value is 8. You can omit the parameter name (-Length) if you place the parameter argument immediately after the script's name on the command line.

-LowerCase, -UpperCase, -Numbers, and -Symbols are switch parameters. All four specify the character classes to include in the random strings. -LowerCase is enabled by default, so if you want to create random strings that do not contain lowercase characters, you must specify

```
-LowerCase:$False
```

All these character classes are based on ASCII characters and are not locale-specific.

The -Count parameter specifies how many random strings to output (1 is the default). For example,

```
-Count 10
```

outputs 10 random strings.

For more information about the script's parameters as well as some sample commands, use

```
Get-Help Get-RandomString -Detailed
```

or

```
Get-Help Get-RandomString -Full
```

Rather than specifying character classes that *might* appear in the password strings, I wanted to specify classes that *will* appear in the password strings.

How Does It Work?

The script begins by declaring a param statement that specifies the script's parameters. All the parameters are declared with default

values. Next, the script determines the -Length parameter argument. If the argument is less than 4, the script throws an error. (Strings must be at least 4 characters because that's the number of available character classes.) As a final sanity check, the script makes sure that at least one of the four character classes (i.e., -LowerCase, -UpperCase, -Numbers, or -Symbols) is included. If none of the four character classes are specified, the script throws an error.

Next, the script declares a set of bitmap mask values that represent the four character classes. (For more information about how bitmaps and masks work, see the sidebar "Bitmaps As Arrays.") The script then creates four arrays that contain the character values for each of the four character classes, based on the ASCII values of the

Bitmaps As Arrays

A *bitmap* is a number that the programmer interprets as an array of Boolean values (i.e., each bit in the number represents a Boolean). You can check and change the bits in a bitmap by using a mask value that represents one or more bit positions in the bitmap. The Get-RandomString.ps1 script uses two numbers as bitmaps. The first bitmap, $charSets, stores the character classes (i.e., lowercase, uppercase, numbers, or symbols) that the user specified on the command line. The second bitmap, $flags, contains the character classes that the randomly generated string actually contains. If the bitmaps don't match, the script generates another random string. You can use the formulas in Table A to check and change the bits in a bitmap. ■

InstantDoc ID 142063

Table A: Formulas for Checking Bits

Purpose	Formula
Check whether at least one bit in the mask is set	`(bitmap -band mask) -ne 0`
Check whether all of the bits in the mask are set	`(bitmap -band mask) -eq bitmap`
Check whether none of the bits in the mask are set	`(bitmap -band mask) -eq 0`
Set the bits specified in the mask	`bitmap = bitmap -bor mask`
Clear the bits specified in the mask	`bitmap = bitmap -band (-bnot mask)`
Toggle the bits specified in the mask	`bitmap = bitmap -bxor mask`

characters. For example, the $charsLower array contains ASCII lowercase characters (i.e., each element in the array is a lowercase ASCII character); the $charsNumber array contains ASCII number characters. The characters that I chose for the $charsSymbol array don't include any characters that might cause problems from the command line (e.g., single and double quotes, pipe and redirection symbols).

After this, the script creates an array, stored in the $charList variable, that contains all the characters from the character classes that are specified on the command line. For example, if -LowerCase and -Numbers exist on the command line, then the $charList variable will contain the characters from both the $charsLower and the $charsNumber arrays. The script also defines the $charSets variable, which is a bitmap value that stores the character sets that have been selected.

The script then defines the test-stringcontents function, which Listing 1 shows. This function uses two parameters: a string and an array of characters. The function returns $True if the string contains at least one character from the array; otherwise, the function returns $False. The script uses this function later to determine whether a random string contains characters from a specified character class.

Listing 1: The test-stringcontents Function

```
function test-stringcontents([String] $test, [Char[]] $chars) {
  foreach ($char in $test.ToCharArray()) {
    if ($chars -ccontains $char) { return $TRUE }
  }
  return $FALSE
}
```

Download

Download the code

After defining the test-stringcontents function, the script loops the number of times that the -Count parameter requests. Next, the script initiates a do loop that generates a random string and checks if the string contains all of the requested character classes. In the do loop,

the script creates the $flags variable (a second bitmap value) to keep track of matching character classes. Then, the script uses the Get-Random cmdlet to append a randomly selected character from the $charList array as many times as the -Length parameter requests, as Listing 2 shows.

Listing 2: Code that Generates a Random String

```
$output = ""
1..$Length | foreach-object {
  $output += $charList[(get-random -maximum $charList.Length)]
}
```

After running the code in Listing 2, the random string contains characters that are randomly selected from the $charList array. However, this doesn't mean that the string is guaranteed to contain characters from each selected character class. To make sure that the string contains at least one character from each class, the script uses the test-stringcontents function (see Listing 1). If the string contains at least one character from a class, it sets the corresponding bit for that class in the $flags bitmap. If the $flags bitmap doesn't match the $charSets bitmap, then the randomly generated string does not contain all the requested character classes, and the *do* loop repeats. Otherwise, the script outputs the string.

Random Password Generation Made Easy

The Get-RandomString.ps1 script uses PowerShell's Get-Random cmdlet and its powerful array- and string-handling functionality to return random strings. You can use the script to create random passwords, PIN codes, or whatever else you need. ■

InstantDoc ID 142062

Product News for IT Pros

NETIKUS.NET Releases EventSentry 2.93.1

NETIKUS.NET released EventSentry 2.93.1, a major new version of its comprehensive monitoring and compliance solution. It features easier installation and deployment, a built-in SQL Server database, improved usability of the management console, an optimized event log monitoring engine, completely redesigned performance monitoring, additional server hardware inventory options, and many other enhancements. The new version features a built-in PostgreSQL-based database, which makes initial setup and deployment easier, especially for new users. The user experience has also been improved in the management console, with better keyboard and mouse navigation as well as significantly improved speed when saving. Performance monitoring, an extremely popular feature in EventSentry, was rewritten and offers new functionality such as trend detection, alert suppression, counter combinations, and more. For more information, check out the NETIKUS.NET website.

Chinook Communications Introduces Hosted Lync and Enterprise Voice Integration for Microsoft Office 365

Chinook Communications announced the introduction of a new service that lets small-to-midsized businesses (SMBs) easily integrate enterprise voice and other hosted Lync services with Exchange Online Unified Messaging hosted by Microsoft Office 365. The new service, Total Connect for Office 365, is designed for businesses seeking to maximize the productivity and cost benefits of hosted unified messaging with integrated, cloud-based phone service. Total Connect for Office 365 includes the full support of Exchange Online Unified Messaging, including voicemail, voice-to-text translation, and Outlook

voice access. In addition to extensive voice capabilities, including public switched telephone network (PSTN), inbound and outbound calling, response groups, call hold, forward and transfer, and simultaneous ring, Lync will provide secure instant messaging (IM), presence, audio conferencing, online conferencing, video conferencing, desktop sharing, and white boarding. To learn more, see the Chinook Communications website.

Devolutions Launches Enhanced Remote Desktop Manager 7.5

Devolutions launched version 7.5 of Remote Desktop Manager, which empowers users to add, edit, delete, share, organize, find, and manage all of their remote connections and virtual machines (VMs). They can also access password management and credentials management features, which improve efficiency and reduce risk. New features in Remote Desktop Manager 7.5 include ScreenConnect integration, inventory reporting, a VMware console with integrated remote control, a credentials dashboard, a session shortcut feature, support for multiple monitors, and multi-installation path support for Putty, TeamViewer, and Dameware. Remote Desktop Manager 7.5 also includes several security enhancements (new security rights, views, and access reports) and VPN improvements (VPN routing, Microsoft VPN connect detection). For more information, visit the Devolutions website.

Napatech Introduces IP Fragmentation Support

Napatech announced new functionality to intelligently identify fragmented IP packets. Available on the latest Napatech network adapters, it provides OEM vendors with a powerful offload tool to increase performance in networks with many fragmented packets. The IP fragmentation feature is the latest addition to the comprehensive, common feature set provided by Napatech on all 1Gbps, 10Gbps, and 40Gbps network adapters. It's the latest addition to a range of intelligent

frame processing, flow identification, and distribution features that help OEM vendors of network appliances offload data processing and focus on data analysis. "IP reassembly is often the first step required before any IP data analysis can be performed," says Napatech CEO Henrik Brill Jensen. "With this feature enhancement, we can help increase performance and enable new features to be implemented as more processing power is freed up for the application." For more information, see the Napatech website.

Nexsan Shipping Storage Systems with 4TB HGST Enterprise-Class Drives

Nexsan announced the immediate availability of 4TB HGST Ultrastar 7,200rpm enterprise-class drives as an option for all Nexsan NST5000 Unified Hybrid Storage and E-Series SAN storage systems. The new high-capacity drives are ideal for 24 × 7 enterprise applications such as big data, cloud computing, data warehousing, video-on-demand, disk-to-disk backup, and virtualized computing. The 4TB HGST Ultrastar drives provide significant capacity, reliability, and performance and offer five Advanced Power Management modes for a low-power operation. HGST's Ultrastar five-platter design has been field proven and is the world's first enterprise-class, 4TB, 7,200rpm hard drive with a 2.0 million hours MTBF specification. The drives have a greater areal density for 33 percent more capacity and 24 percent lower watts-per-gigabyte than earlier 3TB models. To learn more about Nexsan products and news, check out the Nexsan website.

SpydrSafe Launches Beta of SpydrSafe Mobile DLP

SpydrSafe Mobile Security launched the beta of the first mobile security platform that protects corporate data on smart mobile devices. The advanced mobile DLP solution, SpydrSafe Mobile DLP, safeguards against data loss with technology that delivers app-level protection on Android smartphones and tablets. "SpydrSafe Mobile DLP addresses the issues created by BYOD by providing enterprise

IT the tools necessary to safeguard data that is accessed and used by mobile apps," says Michael R. Pratt, CEO of SpydrSafe Mobile Security. The SpydrSafe Mobile DLP for Android app is available on either Google Play or Amazon Appstore for Android. To learn more, visit the SpydrSafe Mobile Security website.

ENow Releases ForeSite

ENow announced the release of ForeSite, a Microsoft SharePoint management solution. ForeSite helps organizations proactively monitor their SharePoint infrastructure, including all of the core underlying technologies such as Microsoft Active Directory (AD), IIS, and SQL Server. It also helps administrators monitor SharePoint's key components, including site availability, timer jobs, and content databases. ForeSite also includes a suite of reports that help administrators better understand how SharePoint is being used in their environment. These reports can be used for planning and capacity purposes. ForeSite is built on top of the ENow Management System platform, which features a customizable dashboard with red, yellow, and green lights indicating the health of each monitored server. ENow's Management System platform is popular for its customizable reporting, which gives administrators complete flexibility in not only how they create reports but also how they disseminate the information. For more information, go to the ENow website. ■

Veeam Backup & Replication 6.0

Alan Sugano

is the president of ADS Consulting Group, which specializes in virtualization, networking, custom programming, Microsoft .NET web development, and SQL Server development. He's the author of *The Real-World Network Troubleshooting Manual* (Charles River Media).

Email

Twitter

LinkedIn

Website

Using a virtualization-specific backup solution in a production environment significantly simplifies the restore process, especially for servers that are difficult to restore, such as those running Microsoft Exchange Server, SQL Server, SharePoint, or Visual Studio Team Foundation Server. Because the backup solutions essentially perform an image backup of the virtual machines (VMs), restoring a VM is as simple as restoring the VM's disk files on the host and starting the VM.

I recently tested Veeam Software's Veeam Backup & Replication, which supports both VMware ESX and Microsoft Hyper-V servers. It comes in two editions: Standard and Enterprise. Both editions include backup and replication (local or remote) functionality. Table 1 summarizes the features included with the Standard and Enterprise Editions. The Enterprise Edition costs around 30 percent more than the Standard Edition, but I think that the features in the Enterprise Edition are well worth the additional cost, especially if you run applications such as Exchange, SharePoint, and SQL Server. You can upgrade from the Standard Edition to the Enterprise Edition by paying the difference in price.

Licensing

Veeam Backup & Replication's licensing is based on the total number of physical CPU sockets you have on all your ESX or Hyper-V hosts. If you have six or fewer CPU sockets to purchase for your entire company, you can buy Veeam Essentials, which is sold in two-socket bundles. However, a company can only buy up to three two-socket bundles. If you have more than six total CPU sockets on your ESX or Hyper-V hosts, you must purchase Veeam on a per-socket basis.

Table 1: Features in the Standard and Enterprise Editions of Veeam Backup & Replication

Feature	Standard Edition	Enterprise Edition	Notes
Backup	Yes	Yes	Backs up local and remote VMware and Hyper-V VMs.
Replication	Yes	Yes	Provides both backup and replication in one package.
Hot VM Copy*	Yes	Yes	Provides ad hoc backups and migrations of VMware VMs.
FastSCP	Yes	Yes	Integrates file management into the operator console.
Changed block tracking	Yes	Yes	Tracks changed blocks in VMs to achieve faster incremental backups.
Multiple backup options	Yes	Yes	Backs up over the LAN or from a SAN or hypervisor I/O stack.
Advanced VSS integration	Yes	Yes	Provides the ability to properly quiesce a VM and truncate log files immediately or after a successful backup, which is especially important for VMs running Exchange and SQL Server.
Web UI	No	Yes	Includes a web-based console (Enterprise Manager) from which you can manage multiple Veeam Backup Servers as well as clone and edit jobs.
Synthetic full backup	Yes	Yes	Eliminates the need for periodic full backups by providing a "forever incremental" backup, saving time and space.
Built-in deduplication	Yes	Yes	Deduplicates data, reducing network traffic and storage requirements.
Near-CDP	Yes	Yes	Provides nearly continuous data protection (CDP) at a lower cost than traditional CDP.
vStorage APIs for Data Protection (VADP)*	Yes	Yes	Uses VADP to protect VMware VMs.
1-Click File Restore	No	Yes	Performs file restores.
Catalog of Windows guest files	Yes	Yes	Creates a catalog of backed-up Windows guest files.
Search across backups	Yes	Yes	Searches Windows guest files in backups. Can search current and archived backups in Enterprise Edition. Can search only the current backup in Standard Edition.
Wizard-driven recovery	Yes	Yes	Includes wizards for instant file recovery in 15 commonly used Windows, Linux, UNIX, Sun Microsystems Solaris, and BSD file systems.
Temporary Spare*	Yes	Yes	Starts a failed VM directly from a backup file.
Full restore with zero downtime*	Yes	Yes	Starts a VM directly from backup storage, then moves the VM to production storage.
Full restore during maintenance window*	Yes	Yes	Minimizes downtime by migrating the VM from backup to production storage.
Universal Application-Item Recovery (U-AIR)*	No	Yes	Provides object-level recovery for any application on any OS using existing application management tools.
User-directed recovery*	No	Yes	Lets users recover their files. Is available for any application with a web front end, such as SharePoint or Salesforce.
Exchange wizard*	No	Yes	Recovers individual Exchange items, such as email messages and contacts.
Active Directory (AD) wizard*	No	Yes	Recovers individual AD objects, such as users and groups.
SQL Server wizard*	No	Yes	Recovers individual SQL Server objects, such as tables and records.
Recovery verification*	No	Yes	Verifies recoverability of backups.
Working copy of production environment*	No	Yes	Creates a working copy of the production environment for troubleshooting, testing, and training in an isolated environment.

* Available for VMware only

You have two options. You can purchase Veeam Backup & Replication as a standalone product or as part of the Veeam Management Suite, which includes Veeam Backup & Replication and Veeam ONE (Veeam's monitoring, documentation, and business categorization application). Veeam Essentials also includes Veeam ONE.

Components

Veeam Backup & Replication consists of several components:

- Veeam Backup Server. This is the main software that schedules and performs the backups.
- Veeam Backup Enterprise Manager. This software provides centralized management of multiple Veeam Backup Servers. You need only one instance of Enterprise Manager to manage multiple servers.
- Veeam Backup Search. Used in conjunction with Microsoft Search Server, Veeam Backup Search is used for offline system catalog crawls and searches. If you have more than 200 VMs, you'll have much faster search results with this software when the file to restore might be located on multiple backups.

From this point on, I'll concentrate on the main features of the Veeam Backup Server component running in a VMware environment.

Installation and Configuration

Although you can install the Veeam Backup Server software on a VM, I suggest that you install it on a dedicated physical server because when the software is running, it places a significant load on the server. Veeam suggests a server with at least two cores and 4GB of memory if you plan to use a local SQL Server instance. If you're using a remote SQL Server instance, you can configure the server with 2GB of memory.

The installation of the Veeam Backup Server software is straightforward. Because the backup server must communicate with either a vCenter server or ESX host, the backup server should be placed in

Editor's Note

Since this product review was written, Veeam Software released Veeam Backup & Replication 6.1. See the sidebar "What's New in Veeam Backup & Replication 6.1" for the details.

the same network as the vCenter server or ESX console network. Ideally, this should be a separate dedicated management network that's isolated from other VM traffic.

Before you run the installation program, you should verify that valid entries exist for all vCenter servers, ESX hosts, and the backup repository (which I'll discuss shortly). These entries can reside either in a DNS server or local HOSTS file on the backup server. Make sure that all resources (vCenter servers and ESX hosts) can be resolved.

For me, the installation of the Veeam Backup Server went very smoothly. When you run the installation program, make sure you have at least 10GB of free space on the drive on which you install vPower NFS. This technology enables running VMs directly from backup files.

After the software is installed, you need to create the backup repository. This is where the backup files, copies of VMs, and metadata for replicated VMs will be stored. The backup repository can be DAS on a server, NAS, NFS storage on a Linux server, or Just a Bunch of Disks (JBOD). I also recommend that you back up the backup repository to some type of offline media, such as tape. I typically run a full backup of the VMs over the weekend and run incremental backups to disk during the week. After the daily backups are finished, I run a separate backup job to tape.

When planning for disk space, make sure to account for the total amount of disk space that your VMs use, plus space for the incremental backups. Veeam does a good job with compression and deduplication of the backup images to save space, but to be on the safe side, I recommend purchasing at least 1.5 times the amount of storage on the host or cluster. More storage lets you keep more backup history on disk, without having to restore from tape.

Backups

Once the Veeam Backup Server software is installed and the backup repository is in place, you can create the backup job. To do so, you

can use the Create Backup Job wizard, which you launch from the initial backup screen that Figure 1 shows. For testing purposes, I configured a full backup on Saturday, with incremental backups Sunday through Friday. If desired, you can have email notifications sent when the backup job has finished. To do so, you just need to specify an SMTP server and the recipients' email addresses, separated by semicolons.

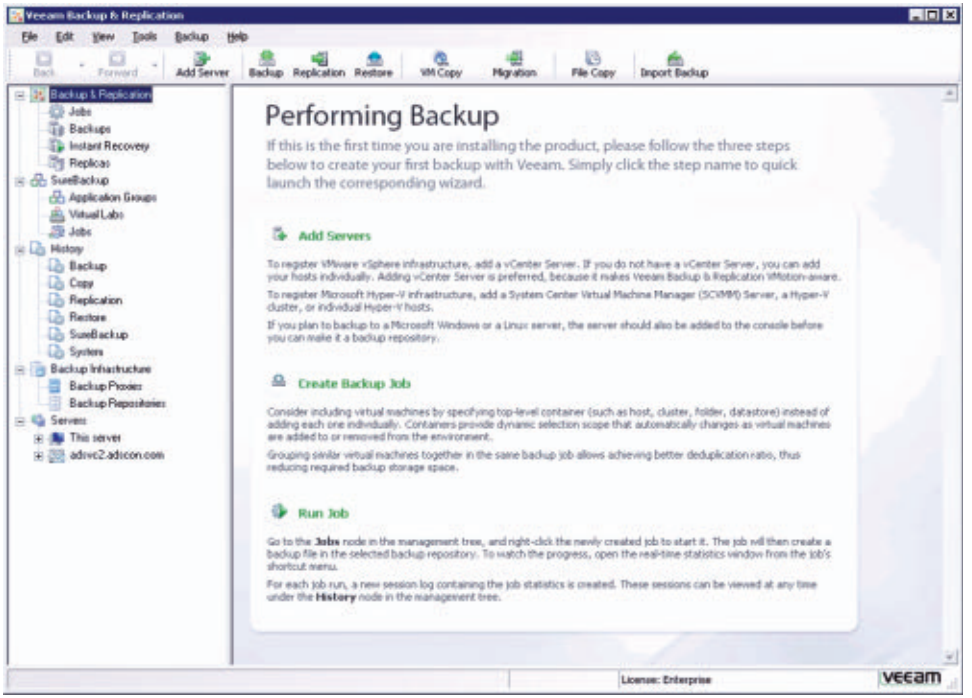


Figure 1
Initial backup screen

In the past, I struggled with other virtualization backup solutions when trying to back up Windows Server 2008 R2 VMs running Exchange and SQL Server on a VMware vSphere 5 host with Virtual Machine File System 5 (VMFS5) storage groups. I had to contact technical support multiple times to get the backup jobs working, with sometimes clunky workarounds. In stark contrast, I was able to get Veeam Backup & Replication working on the first try, without contacting technical support. It was fast, reliable, and stable.

Veeam Backup & Replication is fast, reliable, and stable.

Veeam Backup & Replication 6.0

PROS: Basic installation is simple; backups worked reliably every time

CONS: Getting the Virtual Labs to install and work for granular restores of Exchange, SQL Server, SharePoint and other web applications when the ESX server has a dedicated management network was tricky and required a call to Veeam Technical Support

RATING: ★★★★★

PRICE: Cost based on the total number of CPU sockets and version; for example, costs $1,300 per two sockets for Veeam Essentials Enterprise Edition (includes Veeam Backup & Replication and Veeam ONE; is for companies with six CPUs or fewer) and $1,099 per socket for the standalone Veeam Backup & Replication Enterprise Edition (for companies with more than six CPUs)

RECOMMENDATION: If you have ESX or Hyper-V hosts running production VMs, you need this product. In my opinion, it's the best backup solution available for ESX or Hyper-V.

CONTACT: Veeam Software • 678-353-2140

For my tests, I installed Veeam Backup Server on both a VM and a physical server running VMware vCenter Server to compare the performance. The VM was running Server 2008 R2 configured with four virtual CPUs (vCPUs) and 4GB of memory. When backing up the other VMs on the same ESXi host, the CPU utilization stayed close to 100 percent. Throughput was good, running about 70MBps during a full backup. The host was an HP ProLiant DL380 G7 with two six-core CPUs and 64GB of memory. The backup repository was on the local VM's hard drive. This standalone ESX host had eight 300GB Serial Attached SCSI (SAS) drives configured as a RAID 5 array.

The physical server was an HP ProLiant ML370 G5 with 40GB of memory and two quad-core processors. The backup repository was DAS, consisting of eight 146GB SAS drives configured as a RAID 5 array. CPU utilization averaged at 60 percent, but throughput was noticeably lower at around 48MBps during a full backup. The slower throughput was probably due to the fact that the data was transferred over a single Gigabit Ethernet link.

Veeam supports restoring individual files from a .vmdk image backup. However, Windows VMs with dynamic disks aren't supported. If you have VMs with dynamic disks, you can either migrate the data to a basic disk or convert the disk from dynamic to basic using a partition utility such as EaseUS Partition Master. Before you perform any type of conversion, make sure to get a good backup of the disk to prevent data loss in case a problem occurs.

A No-Fuss Solution

A backup solution should work every time with no fuss. I was so impressed with Veeam Backup & Replication that I replaced my existing virtualization backup solution with it. In addition, I now recommend it to my clients as the preferred backup solution in a vSphere 5 environment. I can't think of a stronger recommendation than that. ■

InstantDoc ID 143213

What's New in Veeam Backup & Replication 6.1

At press time, Veeam had released Backup & Replication 6.1. Here's what the new edition adds to the functionality described in this review.

- VeeamZIP—Ad-hoc backup of a running VM for operational, archival, or portability purposes. For example, admins can now back up a VM before applying patches, create an archive copy of a VM, or copy a VM to a remote test lab, all without powering off the production VM.
- Instant file-level recovery—Users can now restore individual guest files directly from an image-level backup.
- Quick migration for VMware—Migrate a running VM to any host or data store, even if you don't use clusters or shared storage.
- vPower and instant VM recovery for Hyper-V—Enables IT to boot and run a VM directly from a compressed, deduplicated backup file, in a matter of minutes, so businesses can continue without disruption during the restore of the VM back into the production environment.
- SCVMM 2012 support—Extends support for System Center Virtual Machine Manager 2008 R2 to System Center 2012 Virtual Machine Manager. SCVMM support streamlines discovery and ensures protection of VMs managed by SCVMM.
- Updated UI and additional enhancements—The updated UI (enhanced based on user requests and Veeam R&D innovation) is an evolution, not a complete redesign. Current users will still be able to use all their existing jobs and settings; the workflow for the wizards hasn't changed.

Also, Veeam Backup & Replication 6.1 introduces a new free version: Veeam Backup Free. This free mode supports Hyper-V and vSphere, and is a successor to Veeam's first free product, FastSCP. It provides a subset of the functionality in the full version of Veeam Backup & Replication, including VeeamZIP, and VM and file recovery. ■

ZENworks Application Virtualization 9.0

Russell Smith

is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista and XP* (Packt).

Email

Twitter

In a vein similar to Microsoft's Application Virtualization (App-V) and VMware's ThinApp, Novell's ZENworks Application Virtualization 9.0 is a solution for packaging programs into a single self-contained executable that can be run without any special privileges in a virtual "bubble" that isolates the application from the OS and other programs. ZENworks also provides a means for users to stream virtual applications from the Internet or a network share. Streaming an application is similar in concept to how videos load on sites such as YouTube—users can start using the core application features while the remaining code downloads in the background.

Although ZENworks shares some common methodologies with App-V, one major technical difference between the two products is how applications are virtualized. ZENworks relies on before-and-after snapshots of a PC to determine the differences and create a package, whereas App-V monitors an application's native installer to create a package.

When I launched the ZENworks UI, which is referred to as the studio, the configuration wizard offered to scan the PC's desktop for installed applications, which can be packaged using a readymade "recipe," (i.e., a set of predetermined actions required to successfully virtualize a physical application). The wizard detected Adobe Acrobat Reader 10.1, but I was a little surprised to find that none of my Microsoft Office 2010 suite applications were detected for reasons I'll reveal later. Nevertheless, I decided to go ahead and package Acrobat Reader. ZENworks contacted an online server for the latest recipes and proceeded to package the application after I chose the destination directory. Once that was completed, I ran the virtual package and Acrobat Reader started and worked without any problems, as if I had installed the physical application on the PC.

Alternatively, the wizard offers a list of templates that you can use to package commonly used applications. There were many templates for Adobe programs in the list, and I was surprised to find templates for Office 2010 applications—but they supported only the 64-bit versions. That's likely why my Office applications weren't detected when my PC was scanned; per Microsoft's recommendation, I have the 32-bit versions installed because I don't need to address large memory spaces using any of the suite programs. The lack of support for x86 Office seems to be a rather odd omission on Novell's part.

The lack of support for x86 Office seems to be a rather odd omission on Novell's part.

Despite previous bad experiences with before-and-after snapshots to create installer packages in other applications, I decided to try this technique to package the Citrix Systems GoToMeeting client. In retrospect, this probably wasn't the best candidate for this test, but it's a relatively simple application. I used the handy wizard, making a few simple decisions along the way, such as which file format to use and the output directory. Unfortunately, the resulting package wouldn't even launch, with no indication of what the problem was or whether something had gone wrong in the snapshot process.

Advanced Features

The ZENworks studio includes support for adding runtimes to a package. So, if your developers are working on a .NET application, they can use the studio's Runtimes tab to select the correct version of the Microsoft .NET Framework (up to version 4.0) and have all the necessary library files added to the package. When the virtual application is launched, there's no requirement for the .NET Framework to be preinstalled on the client PC. Runtimes are also available for Java, Adobe Flash Player, Adobe Shockwave Player, and Microsoft SQL Server 2005 Express Edition. (There's no support for the newer versions of SQL Server.)

Modifying my packages' file and registry entries in the studio was easy. I could also add files and registry keys as necessary if they had been missed for whatever reason. Other settings are also easily edited,

ZENworks Application Virtualization 9.0

PROS: Includes support for .NET and Java-based applications; no server required for streaming virtual applications

CONS: Snapshot capture of applications is less than reliable; streaming and management not as comprehensive as that in some competing products

RATING: ★★½☆☆

PRICE: Starts at $39 for a single license

RECOMMENDATION: ZENworks Application Virtualization is useful for creating virtual applications that run without any OS dependencies. However, it's difficult to use if you need to virtualize internal line of business (LOB) applications and you don't have prior experience in creating installer packages.

CONTACT: Novell • 800-529-3400 or 801-861-4272

such as the ability to change whether child processes are spawned in or out of the virtualized environment, which could be important for security and compatibility. After you configure the file, registry, and package settings, they can be exported as a shared component (.svm file) and reused across multiple virtual applications.

In the UI's Setup pane, you can create basic Windows Installer (.msi) packages for virtual applications, without needing to use a database table editor such as Orca.exe. I was able to edit the basic .msi file information, add desktop shortcuts, and file associations.

Although it's not a requirement, you can prevent virtual applications from running if the ZENworks Configuration Management Agent is installed on the client device. The agent gives you more control over which PCs virtual applications can be run on. If you want, you can have the virtual packages automatically expire and create custom messages that warn users a predefined number of days in advance of the expiration.

A Tool for Developers

I tried repeatedly to contact Novell to provide support for this product, but was unable to get a response. My time with ZENworks Application Virtualization and my previous experience of capturing applications using before-and-after snapshots lead me to believe that it's better suited for developers or systems administrators who know how to work with Windows Installer databases and other installer technologies. Anyone who expects that using the snapshot method to virtualize complex applications is an easy, quick option might find that it's actually a time-consuming process or even that they're out of their depth. As such, I can't recommend this application for those people looking for a reliable, user-friendly packaging solution. ■

InstantDoc ID 143173

HP ProBook 5330m

Nobody wants to lug a 10-pound laptop to a business meeting when a sleek 4-pound model will do the job nicely. So, traditional IT hardware vendors such as Dell, HP, and Lenovo are responding to the challenge of providing employees with the mobile devices they need. One of the best attempts yet at a business laptop makeover is the HP ProBook 5330m. Can the ProBook provide an equal dose of style and business productivity? Let's find out.

Jeff James

is a former industry news analyst for *Windows IT Pro*. He also was editor-in-chief of *TechNet Magazine* and was an editorial director at the LEGO Company. Jeff has more than 15 years of experience as a technology writer and journalist.

Email

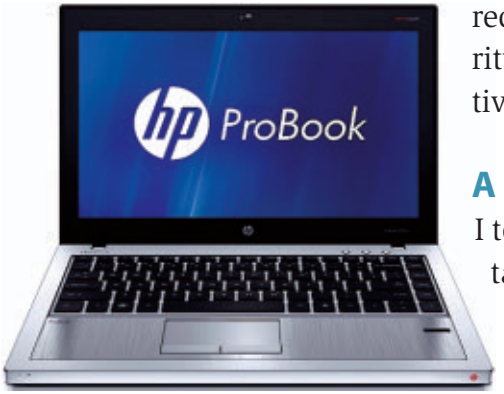
Twitter

Brains and Beauty

The ProBook 5330m I reviewed shipped with a 2.5GHz Sandy Bridge Intel Core i5 processor, 4GB of RAM, a 500GB 7200rpm Serial ATA (SATA) drive, Intel HD Graphics 3000, and Beats Audio technology. The 13" screen (1366 × 768 maximum screen resolution) came covered in a nice anti-glare coating that was easy on the eyes, perfect for prolonged bouts of writing and editing. Three USB 2.0 ports, an Ethernet port, a VGA port, a headphone jack, and an HDMI port rounded out the complement of available ports. Wireless and Bluetooth support were also included.

The laptop is attractively designed but a bit more boxy and utilitarian than more svelte laptops on the market. Most of the laptop case is fashioned out of attractively styled brushed aluminum bits, but the underside has a grippy rubber coating. This underside material makes the laptop firmly plant itself on a variety of surfaces, which can be a benefit for people with vigorous typing styles.

This particular ProBook tips the scales at just under 4 pounds and comes equipped with a Trusted Platform Module (TPM) and Intel's vPro technology. Other noteworthy IT-friendly features include the 64-bit version of Windows 7 Professional and HP's ProtectTools suite of security software. This suite handles hardware encryption, facial



recognition as a password replacement, and other security features that could make this laptop a more attractive buy for IT pros in security-minded industries.

A Day in the Life

I tested the ProBook 5330m for several weeks, including taking it to several trade shows and other work-related events. I found the battery life to be fairly good, averaging three to four hours when I was primarily using the laptop for light-duty tasks, such as editing, writing, and web surfing. The battery life was understandably less impressive when I was watching videos or performing other more processor-intensive tasks.

Although it's not as lightweight as other laptop offerings, I found the ProBook's weight to be one of the most attractive features, especially when I had to carry the laptop between meetings or trade show briefings. The backlit keyboard worked great in low-light conditions, but I found the laptop keys to be overly noisy and squeaky during use, almost as if they needed a shot of WD-40. I eventually grew accustomed to the noise, but HP might want to revisit the backlit keyboard design in future versions of the laptop. One potential negative for some IT pros is the lack of an internal DVD or Blu-ray drive, but this can be remedied by purchasing an external drive as an accessory.

HP ProBook 5330m

PROS: One of the most stylish Windows business laptops available; backlit keyboard; excellent security and business features

CONS: Saddled with a fair amount of bloatware; hardware design seems half-finished in spots; noisy keyboard keys

RATING: ★★★★☆

PRICE: Starts at $929

RECOMMENDATION: It might not be able to best the ultraportable MacBook Air, but the HP ProBook 5330m is lightweight, attractive, and business-friendly.

CONTACT: HP • 866-625-0242

Big Strides Made

The ProBook offers a compelling combination of being lightweight, having an attractive exterior design, and offering business-friendly features. Although the ProBook might not have the goods to best the Apple MacBook Air and other ultraportable laptops and mobile computing devices, HP has made big strides with it. I'm looking forward to what the company might do for an encore. ■

InstantDoc ID 143725

Insights from the Industry

Microsoft Study Attempts to Dispel Cloud Security Concerns

Concerns about cloud security have helped dampen enthusiasm for cloud computing among some IT professionals, a perception that Microsoft hopes to reverse with some findings from a study it recently commissioned. The study was conducted in India, Hong Kong, Malaysia, Singapore, and the United States. Study participants consisted of small-to-midsized businesses (SMBs) that were using (and not using) cloud services. Microsoft has released the US survey results and plans to release results from other countries in the future.

I spoke with Tim Rains, director at Microsoft Trustworthy Computing, and he suggested that the survey results prove that security—rather than being a negative for cloud computing adoption—is actually turning into a positive for cloud computing adopters. "This study shows that businesses that use the cloud get savings in time and money, but they also get increased levels of security," Rains said. "Security [concerns] have been a barrier to cloud adoption, but the study shows that users are gaining security rather than losing it."

A Microsoft statement outlines some of the key findings of the study, namely:

> The study shows that 35 percent of US companies surveyed have experienced noticeably higher levels of security since moving to the cloud. In addition, 32 percent say they spend less time worrying about the threat of cyberattacks. US SMBs

Jeff James

is a former industry news analyst for *Windows IT Pro*. He also was editor-in-chief of *TechNet Magazine* and was an editorial director at the LEGO Company. Jeff has more than 15 years of experience as a technology writer and journalist.

Email

Twitter

using the cloud also spend 32 percent less time each week managing security than companies not using the cloud. They are also five times more likely to have reduced what they spend on managing security as a percentage of overall IT budget.

For more information on the Microsoft cloud security study, read the TechNet blog post "Barrier or Benefit? Study Challenges Cloud Computing Security Perceptions for Small to Mid-size Businesses," by Adrienne Hall, general manager at Microsoft's Trustworthy Computing Group, or peruse the details in the Microsoft press release "Cloud Computing Security Benefits Dispel Adoption Barrier for Small to Midsize Businesses."

—Jeff James

InstantDoc ID 143086

B. K. Winstead

is a senior associate editor for *Windows IT Pro*, *SQL Server Pro*, and *SharePoint Pro*, specializing in messaging, mobility, and unified communications.

Email

Twitter

Blog

Mobile Devices Are Transforming Corporate IT

We've been talking about the concept of Bring Your Own Device (BYOD) for some time, so Microsoft Exchange Server admins are well aware of the security and management concerns that the explosion of personal mobile devices has wrought on the corporate network. Now, we're beginning to see other effects of the smartphone revolution ricochet back into the PC world. Let's take a quick look at some of the things Exchange admins and other IT pros should be prepared for with this shift.

A prominent and much talked about example of the smartphone world coming to PCs is the forthcoming Windows 8 and its Metro interface, which is taken from the Windows Phone mobile OS. Although Windows 8 still includes the traditional desktop that we're all familiar with, Microsoft's focus is on the Metro tile-based UI and touch screen accessibility, which lends itself particularly well to tablets. Whatever

you think of Windows 8 and what Paul Thurrott calls these "dueling desktops," clearly Microsoft is taking a cue from Apple's iPad success and the larger influence of the mobile market.

Microsoft isn't the only company that's moving with this trend, of course. Kerio Technologies released an update to its Kerio Connect cross-platform messaging server. The news with Kerio Connect 7.4 is that it's been optimized for management from iPads—that is, you can use your iPad to run your Kerio messaging environment, and you can do it from wherever you have a connection to your corporate network. (Something tells me that iPad optimization isn't a feature Microsoft will be introducing with Exchange 2013.)

The Kerio announcement highlights an aspect of the mobile device shift, namely the desire—or, indeed, the need—to manage corporate systems from tablets or smartphones. In fact, this market isn't entirely new. Several vendors have been addressing this need for a while. Last year, Eric B. Rux reviewed three such products in "Comparative Review: Smartphone-Capable Network Monitoring Solutions." Many other products are out there, and you can probably find something that's optimized for your particular mobile device or network management solution.

As an admin of Exchange Server or other systems, you might frequently find yourself needing to respond to requests or troubleshoot problems when you're not sitting at your workstation. Having mobile access to your systems is increasingly going to be a necessity rather than a nice-to-have. If you're looking at monitoring or management add-ons for Exchange, you might want to keep in mind which of those products will provide the best mobile access story. It might also help determine which smartphones or tablets your IT department purchases for its own use.

One of the most interesting developments I've seen for PCs that can be traced back directly to smartphones comes from Embarcadero Technologies. Taking a cue from mobile platform app stores, Embarcadero has launched the AppWave Store, which delivers apps

to PCs in a fashion that's similar to the way mobile devices download and run apps. The store launched last month with a wide array of familiar productivity and business apps that are ready to go. It also features plenty of well-known multimedia and entertainment apps (i.e., games) that smartphone addicts will no doubt be familiar with (e.g., Angry Birds).

"Essentially what we're doing is taking the Windows application and we're delivering it to the user as a pre-installed image," said Michael Swindell, senior vice president of marketing and product management for Embacadero. "So there's no installation process. Everything that's needed to run the application is pulled down in one image and cached locally on the user's machine. It acts and works as if it's installed. Really, the user wouldn't know any difference."

Swindell used a garden metaphor to explain how this works. In a thriving garden, trees and plants interact happily above ground while below ground their roots might be competing critically for resources. That below-ground part is what happens at the OS level on the PC when you install and run multiple applications. With the AppWave Store model, you're able to put each app/plant in its own pot so its roots are completely self-contained and it doesn't have to compete for resources. Essentially, this model is what the mobile OSs have been able to do—after seeing the difficulties and conflicts of running applications on PCs.

"For a long time you saw mobile devices trying to emulate a more traditional computer experience," Swindell said. "You see a divergence say in the last 5 to 6 years with iPhone and others trying to create a phone experience. In some ways, what we're doing is trying to manipulate that mobile experience and just simplify the discovery and acquisition of software for PCs." The AppWave Store requires you to download its own browser to manage the apps, but all the apps currently available are free—and fun to try out.

So what about BYOD itself? Are you still struggling with managing employee-owned devices in your environment? Or have you locked

everything down and have it under control? Paul Robichaux has a really interesting take on this problem, which essentially places it in the overall evolution of technology that's a constant that IT departments have had to deal with and will continue to deal with. As Paul points out, you can find third-party products to help with mobile device management (MDM) if necessary.

It's important to remember what your workers, and therefore your business, gain by letting employees access corporate email and other resources via their mobile devices. "You've now turned your worker, who used to be 9 to 5, into someone that is proactively saying, 'Actually, you can reach me any time via email, or whatever the message type happens to be.' So you've got that productivity gain," said Martin Brewer, director of research and development for Wavelink, who makes the MDM solution Wavelink Avalanche.

Although I'm not an advocate for people working excessive hours or being on call 24 × 7, I can personally vouch for how having a smartphone with company email has changed my work habits and my personal expectations for how I should be available and respond to issues at work. As Brewer said, "You want to walk that fine line to ensure people want to proactively bring their device, use their device, and be more productive from a mobile standpoint, without trying to limit what they can do to an unnecessary degree."

All projections seem to point to continued growth in the smartphone market. Tablets are becoming the new PC for many people. So it's fair to say this amalgamation of platform types is only likely to continue. It's certainly worth keeping in mind how smartphones, tablets, and PCs interact when you consider how best to manage your environments, and take advantage of those changes that make sense. ■

—B. K. Winstead

InstantDoc ID 143200

Jason Bovberg

Email

Twitter

Website

What Are Your Favorite Products?

Every year, in our December issue, we present our Editors' Best and Community Choice awards. The Editors' Best awards are given to products that *Windows IT Pro* editors and authors believe are the best-of-breed products in their respective categories. We evaluate the products based on their strategic importance to the market, competitive advantages, and value to the customer. However, it's our Community Choice awards that really give you, our readers, an opportunity to make your voice heard about your favorite products on the market.

At our Awards Central hub on the *Windows IT Pro* website, you can find information about all our awards programs, including our show-based Best of TechEd and Best of Connections awards, as well as our Editors' Best and Community Choice awards. Click on our Community Choice page to find information about the nominating and voting processes. Don't miss your chance to cast your votes! Final voting for this year's Community Choice awards is happening now!

Send us your funny screenshots, oddball product news, and hilarious end-user stories. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube.

Submit

Directory of Services

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

- Cloud & Virtualization UPDATE
- *Dev Pro* UPDATE
- Exchange & Outlook UPDATE
- Security UPDATE
- *SharePoint Pro* UPDATE
- *SQL Server Pro* UPDATE
- *Windows IT Pro* UPDATE
- WinInfo Daily UPDATE

RELATED PRODUCTS

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
www.windowsitpro.com/go/vipsub

SQL Server Pro

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

Dev Pro

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

Advertiser Directory

Vendor Directory

Windows IT Pro